vmware by Broadcom

VMware vSphere 7.0

Table of Contents

Release Notes **75**
VMware vSphere 7.0 Release Notes **75**
VMware vCenter Server Photon OS Security Patches **96**
ESXi Update and Patch Release Notes **110**
VMware ESXi 7.0 Update 3w Release Notes 110
VMware ESXi 7.0 Update 3v Release Notes 140
VMware ESXi 7.0 Update 3s Release Notes 216
VMware ESXi 7.0 Update 3r Release Notes 246
VMware ESXi 7.0 Update 3q Release Notes 277
VMware ESXi 7.0 Update 3p Release Notes 336
VMware ESXi 7.0 Update 3o Release Notes 366
VMware ESXi 7.0 Update 3n Release Notes 431
VMware ESXi 7.0 Update 3m Release Notes 461
VMware ESXi 7.0 Update 3l Release Notes 491
ESXi Release Notes Before Mar'23 546
vCenter Server Update and Patch Releases **634**
VMware vCenter Server 7.0 Update 3w Release Notes 634
VMware vCenter Server 7.0 Update 3v Release Notes 662
VMware vCenter Server 7.0 Update 3u Release Notes 694
VMware vCenter Server 7.0 Update 3t Release Notes 722
VMware vCenter Server 7.0 Update 3s Release Notes 724
VMware vCenter Server 7.0 Update 3r Release Notes 752
VMware vCenter Server 7.0 Update 3q Release Notes 781
VMware vCenter Server 7.0 Update 3p Release Notes 819
VMware vCenter Server 7.0 Update 3o Release Notes 847
VMware vCenter Server 7.0 Update 3n Release Notes 882
VMware vCenter Server 7.0 Update 3m Release Notes 910
VMware vCenter Server 7.0 Update 3l Release Notes 938
vCenter Release Notes Before Mar'23 971
VMware Host Client Release Notes **972**
VMware Host Client 1.37.0 Release Notes 972
VMware Host Client 1.34.8 Release Notes 973
VMware Host Client 1.34.4 Release Notes 975
VMware Host Client 1.34.0 Release Notes 976
ESXi Installation and Setup **978**
ESXi Installation and Setup **978**

About VMware ESXi Installation and Setup....978
Introduction to vSphere Installation and Setup....978
Overview of the vSphere Installation and Setup Process....979
About ESXi Evaluation and Licensed Modes....980
Installing and Setting Up ESXi....980
ESXi Requirements....980
ESXi System Storage Overview....980
ESXi Hardware Requirements....983
Supported Remote Management Server Models and Firmware Versions....986
Recommendations for Enhanced ESXi Performance....986
Incoming and Outgoing Firewall Ports for ESXi Hosts....987
Required Free Space for System Logging....988
VMware Host Client System Requirements....988
ESXi Passwords and Account Lockout....988
Preparing for Installing ESXi....990
Download the ESXi Installer....990
Options for Installing ESXi....991
Media Options for Booting the ESXi Installer....992
Using Remote Management Applications....996
Customizing Installations with vSphere ESXi Image Builder....996
Required Information for ESXi Installation....1030
Installing ESXi....1031
Installing ESXi Interactively....1031
Installing or Upgrading Hosts by Using a Script....1033
Overview of the Network Boot Installation Process....1047
Installing ESXi Using vSphere Auto Deploy....1057
Troubleshooting vSphere Auto Deploy....1125
Setting Up ESXi....1130
ESXi Autoconfiguration....1130
About the Direct Console ESXi Interface....1130
Enable ESXi Shell and SSH Access with the Direct Console User Interface....1133
Managing ESXi Remotely....1134
Set the Password for the Administrator Account....1134
Configuring the BIOS Boot Settings....1134
Configuring Network Settings....1135
Storage Behavior....1141
Configuring System Logging....1142
Set the Host Image Profile Acceptance Level....1153
Remove All Custom Packages on ESXi....1154
Modify ESXi Configuration Files....1154

Deactivate Support for Non-ASCII Characters on ESXi....1154
Reset the System Configuration....1155
After You Install and Set Up ESXi....1155
Licensing ESXi Hosts....1155
View System Logs....1156
Troubleshooting ESXi Booting....1157
Host Stops Unexpectedly at Bootup When Sharing a Boot Disk with Another Host....1157
Host Fails to Boot After You Install ESXi in UEFI Mode....1157
Decommission an ESXi Host....1158
ESXi Upgrade....1159
About VMware ESXi Upgrade....1159
vCenter Server Upgrade Options....1159
Overview of the vSphere Upgrade Process....1159
Overview of the ESXi Host Upgrade Process....1160
Upgrading Virtual Machines and VMware Tools....1162
Upgrading ESXi Hosts....1163
ESXi Requirements....1163
ESXi System Storage Overview....1163
ESXi Hardware Requirements....1165
Supported Remote Management Server Models and Firmware Versions....1168
Recommendations for Enhanced ESXi Performance....1168
Incoming and Outgoing Firewall Ports for ESXi Hosts....1169
Required Free Space for System Logging....1170
VMware Host Client System Requirements....1170
ESXi Passwords and Account Lockout....1170
Before Upgrading ESXi Hosts....1172
Upgrading Hosts That Have Third-Party Custom VIBs....1173
Upgrading ESXi Hosts in an Environment With VMware NSX....1173
Media Options for Booting the ESXi Installer....1173
Using Remote Management Applications....1177
Download the ESXi Installer....1177
Storage Device Names and Identifiers....1178
Upgrade Hosts Interactively....1179
Installing or Upgrading Hosts by Using a Script....1180
Enter Boot Options to Run an Installation or Upgrade Script....1180
Boot Options....1181
About Installation and Upgrade Scripts....1182
Install or Upgrade ESXi from a CD or DVD by Using a Script....1192
Install or Upgrade ESXi from a USB Stick by Using a Script....1193
Network Boot the ESXi Installer for a Scripted Installation or Upgrade....1193

Overview of the Network Boot Installation Process 1194
Boot the ESXi Installer by Using PXE and TFTP 1195
Boot the ESXi Installer by Using iPXE and HTTP 1196
Boot the ESXi Installer by Using Native UEFI HTTP 1198
Network Boot Background Information 1200
PXELINUX Configuration Files 1201
Sample DHCP Configurations 1201
Upgrading Hosts by Using ESXCLI Commands 1204
VIBs, Image Profiles, and Software Depots 1205
Understanding Acceptance Levels for VIBs and Hosts 1205
See if ESXi Host Update Requires Maintenance Mode or Reboot 1207
Place a Host in Maintenance Mode 1208
Update a Host with Individual VIBs 1209
Upgrade or Update a Host with Image Profiles 1210
Update ESXi Hosts by Using Zip Files 1212
Remove VIBs from a Host 1212
Add Third-Party Extensions to Hosts with an ESXCLI Command 1213
Perform a Dry Run of an ESXCLI Installation or Upgrade 1213
List the Available VIBs and Profiles After Host Reboot 1214
Display the Image Profile and Acceptance Level of the Host 1214
After You Upgrade ESXi Hosts 1215
About ESXi Evaluation and Licensed Modes 1215
Licensing ESXi Hosts After Upgrade 1215
Run the Secure Boot Validation Script on an Upgraded ESXi Host 1216
Configure Syslog on ESXi Hosts 1216
ESXi Syslog Options 1218
Fine-tune Syslog on ESXi Hosts 1222
Configure Log Filtering on ESXi Hosts 1227
Using vSphere Auto Deploy to Reprovision Hosts 1228
Introduction to vSphere Auto Deploy 1228
Preparing for vSphere Auto Deploy 1230
Prepare Your System for vSphere Auto Deploy 1231
Using vSphere Auto Deploy Cmdlets 1232
Set Up Bulk Licensing 1233
Reprovisioning Hosts 1235
Reprovision Hosts with Simple Reboot Operations 1235
Reprovision a Host with a New Image Profile by Using PowerCLI 1235
Write a Rule and Assign a Host Profile to Hosts 1236
Test and Repair Rule Compliance 1237
Collect Logs to Troubleshoot ESXi Hosts 1238

vCenter Server Installation and Setup....1239

Introduction to vSphere Installation and Setup....1239

Overview of the vSphere Installation and Setup Process....1239

vCenter Server Components and Services....1240

Overview of the vCenter Server Appliance....1242

Understanding vSphere Domains and Domain Names....1242

vCenter Enhanced Linked Mode....1243

vCenter Enhanced Linked Mode for vCenter Server Appliance....1243

Deploying the vCenter Server Appliance....1244

System Requirements for the vCenter Server Appliance....1245

Hardware Requirements for the vCenter Server Appliance....1245

Storage Requirements for the vCenter Server Appliance....1246

Software Requirements for the vCenter Server Appliance....1247

Required Ports for vCenter Server....1247

DNS Requirements for the vCenter Server Appliance....1247

vSphere Client Software Requirements....1248

Preparing for Deployment of the vCenter Server Appliance....1248

System Requirements for the vCenter Server Installer....1248

Download and Mount the vCenter Server Installer....1249

Synchronizing Clocks on the vSphere Network....1250

System Clock Synchronization Between the Client and Server....1250

Prerequisites for Deploying the vCenter Server Appliance....1251

GUI Deployment of the vCenter Server Appliance....1251

Required Information for Deploying a vCenter Server Appliance....1252

Deploy the vCenter Server Appliance by Using the GUI....1255

CLI Deployment of the vCenter Server Appliance....1259

Prepare Your JSON Configuration File for CLI Deployment....1259

Syntax of the CLI Deployment Command....1268

Deploy a vCenter Server Appliance by Using the CLI....1269

Deploy Multiple vCenter Server Appliances Using the CLI....1269

File-Based Backup and Restore of vCenter Server....1270

Considerations and Limitations for File-Based Backup and Restore....1270

Schedule a File-Based Backup....1273

Manually Back up vCenter Server by Using the vCenter Server Management Interface....1274

Restore vCenter Server from a File-Based Backup....1275

Stage 1 - Deploy a New Appliance....1277

Stage 2 - Transfer Data to the Newly Deployed Appliance....1280

Image-Based Backup and Restore of a vCenter Server Environment....1280

Considerations and Limitations for Image-Based Backup and Restore....1280

Restore a vCenter Server Image-based Environment....1283

Restore a vCenter Server Instance....1285
Restore a vCenter Enhanced Linked Mode Environment....1285
After You Deploy the vCenter Server Appliance....1285
Log In to vCenter Server by Using the vSphere Client....1286
Repoint vCenter Server to Another vCenter Server in a Different Domain....1286
Repoint a Single vCenter Server Node to an Existing Domain without a Replication Partner....1286
Repoint a vCenter Server Node to an Existing Domain with a Replication Partner....1289
Repoint a vCenter Server Node to a New Domain....1291
Syntax of the Domain Repoint Command....1293
Understanding Tagging and Authorization Conflicts....1294
vCenter Server Domain Repoint License Considerations....1297
Troubleshooting vCenter Server Installation or Deployment....1297
Collecting Logs for Troubleshooting a vCenter Server Installation or Upgrade....1297
Retrieve Installation Logs Manually....1297
Collect Deployment Log Files for the vCenter Server Appliance....1298
Export a vCenter Server Support Bundle for Troubleshooting....1298
vCenter Server Upgrade....1300
vCenter Server Upgrade Options....1300
Overview of the vSphere Upgrade Process....1300
Overview of the vCenter Server Upgrade Process....1301
vCenter Server Upgrade Compatibility....1303
vCenter Server7.0 Component Behavior Changes That Affect Upgrade....1304
Removal of Platform Services Controller....1305
Upgrade or Migration for vCenter Server Instances with an External Platform Services Controller....1305
Upgrading or Migrating to vSphere License Service....1306
Upgrading the Trust Authority vCenter Server....1306
Differences Between vSphere Upgrades, Patches, Updates, and Migrations....1306
Support for Upgrading a vCenter Server with Multi-Homing....1307
Support for Federal Information Processing Standard 140-2....1307
Support for Transport Security Layer 1.2....1307
Moving from a Deprecated to a Supported vCenter Server Deployment Topology Before Upgrade or Migration....1308
Example Upgrade Paths from vCenter Server 6.5 and 6.7 to vCenter Server7.0....1309
Example Migration Paths from vCenter Server for Windows to vCenter Server 7.0....1310
Upgrading the vCenter Server Appliance....1312
About the Upgrade Process of the vCenter Server Appliance....1313
System Requirements for the vCenter Server Appliance....1314
Hardware Requirements for the vCenter Server Appliance....1314
Storage Requirements for the vCenter Server Appliance....1314
Software Requirements for the vCenter Server Appliance....1315

Required Ports for vCenter Server....1315
DNS Requirements for the vCenter Server Appliance....1316
vSphere Client Software Requirements....1316
Preparing to Upgrade the vCenter Server Appliance....1317
System Requirements for the vCenter Server Installer....1317
Download and Mount the vCenter Server Installer....1318
Synchronizing Clocks on the vSphere Network....1318
Transferring Data After Upgrade or Migration....1319
Prepare ESXi Hosts for vCenter Server Appliance Upgrade....1320
Determine the Oracle Database Size and the Storage Size for the New Appliance....1322
Download and Run VMware Migration Assistant on the Source Update Manager Machine....1324
Prerequisites for Upgrading the vCenter Server Appliance....1324
GUI Upgrade of the vCenter Server Appliance....1326
Required Information for Upgrading a vCenter Server Appliance 6.5 or 6.7....1327
Upgrade a vCenter Server Appliance 6.5 or 6.7 with an Embedded Platform Services Controller by Using the GUI....1331
Upgrade a vCenter Server Appliance 6.5 or 6.7 with an External Platform Services Controller Instance by Using the GUI....1337
Upgrading vCenter Server in High Availability Environments....1342
Prerequisites for Upgrading vCenter Server High Availability Environments....1342
Upgrade a vCenter Server Appliance 6.5 or 6.7 HA Cluster with an Embedded Platform Services Controller by Using the GUI....1343
Upgrade a vCenter 6.5 or 6.7 HA Cluster with an External Platform Services Controller by Using the GUI. 1347
CLI Upgrade of the vCenter Server Appliance....1353
Prepare Your JSON Configuration File for CLI Upgrade....1353
Upgrade a vCenter Server Appliance by Using the CLI....1365
Syntax of the CLI Upgrade Command....1366
Migrating vCenter Server for Windows to Appliance....1368
Overview of Migration from vCenter Server on Windows to vCenter Server Appliance....1368
Migration of Update Manager from Windows to a vCenter Server Appliance 7.0....1370
System Requirements for Migrating vCenter Server Deployments to Appliance Deployments....1370
Pre-migration Checks....1371
Known Limitations....1372
Preparing for Migration....1372
Synchronizing Clocks on the vSphere Network....1372
Preparing vCenter Server Databases for Migration....1373
Prepare Managed ESXi Hosts for Migration....1375
Preparing vCenter Server Certificates for Migration....1376
System Requirements for the vCenter Server Installer....1377
Determine the Oracle Database Size and the Storage Size for the New Appliance....1377

Determine the Microsoft SQL Server Database Size and the Storage Size for the New vCenter Server Appliance....1379
Download and Run VMware Migration Assistant on the Source Windows Machine....1380
Prerequisites for Migrating vCenter Server....1381
Required Information for Migrating vCenter Server from Windows to an Appliance....1383
GUI Migration of vCenter Server with an Embedded Platform Services Controller to an vCenter Server Appliance....1386
Deploy the OVA File for Migrating to the Target vCenter Server Appliance....1387
Set Up the Target vCenter Server Appliance....1391
GUI Migration of vCenter Server with an External Platform Services Controller to an Appliance....1391
Deploy the OVA File for the Target vCenter Server Appliance....1393
Set Up the Target vCenter Server Appliance....1396
CLI Migration of a vCenter Server Installation from Windows to an Appliance....1397
Prepare JSON Configuration Files for CLI Migration....1397
JSON Templates for CLI Migration of vCenter Server for Windows....1398
About Migrating a vCenter Server for Windows with an External Platform Services Controller Using the CLI....1399
Migration Configuration Parameters....1401
Run a Pre-Check Before a CLI Migration to vCenter Server Appliance....1409
Perform a CLI Migration of vCenter Server from Windows to an Appliance....1410
Syntax of the CLI Migrate Command....1411
After Upgrading or Migrating vCenter Server....1412
Verify Your vCenter Server Upgrade or Migration Is Successful....1413
Log In to vCenter Server by Using the vSphere Client....1413
Decommission the Platform Services Controller....1414
Decommission an External Platform Services Controller Appliance....1414
Decommission an External Platform Server Controller for Windows....1415
Identity Sources for vCenter Server with vCenter Single Sign-On....1415
Reregister Plug-In Solution in vCenter Server After Upgrade or Migration....1416
Roll Back a vCenter Server Upgrade or vCenter Server on Windows Migration....1416
Monitor and Manage Historical Data Migration....1416
Managing Software Updates, Upgrades, and Product Compatibility....1417
Monitor Interoperability for the Current vCenter Server Version....1418
Generate an Interoperability Report for Target vCenter Server Versions....1418
Generate Pre-Update Reports....1419
Patching and Updating vCenter Server7.0 Deployments....1419
Patching vCenter Server....1420
Patching vCenter Server Using the vCenter Server Management Interface....1420
Patching the vCenter Server Appliance by Using the Appliance Shell....1424
Patch a vCenter High Availability Environment....1428

Troubleshooting a vSphere Upgrade **1429**
Collect Installation Logs for vCenter Server Appliance 1429
Errors and Warnings Returned by the Installation and Upgrade Precheck Script 1429
Upgrade Issues with vCenter Server Containing Host Profiles 1431
Roll Back a vCenter Server Instance on Windows When vCenter Server Upgrade Fails 1432
Collect Logs to Troubleshoot ESXi Hosts 1433
vSphere Authentication **1434**
Updated Information **1435**
Getting Started with Certificate Management and Authentication **1436**
vSphere Certificate Management and Authentication Overview 1437
Managing Certificates 1438
Manage Certificates from the vSphere Client 1438
Use Scripts to Manage Certificates 1439
Managing Authentication Services 1439
Manage Authentication Services from the vSphere Client 1440
Use Scripts to Manage Authentication Services 1440
Managing the vCenter Server 1440
Manage vCenter Server with the Management Interface 1441
Manage vCenter Server from the vCenter Server Shell 1441
Add a vCenter Server to an Active Directory Domain 1442
vSphere Security Certificates **1442**
Certificate Requirements for Different Solution Paths 1443
Certificate Management Overview 1446
Certificate Replacement Overview 1448
Where vSphere Uses Certificates 1450
VMCA and VMware Core Identity Services 1452
VMware Endpoint Certificate Store Overview 1452
Managing Certificate Revocation 1454
Certificate Replacement in Large Deployments 1454
Managing Certificates with the vSphere Client 1455
Explore Certificate Stores from the vSphere Client 1456
Set the Threshold for vCenter Certificate Expiration Warnings 1457
Renew VMCA Certificates with New VMCA-Signed Certificates from the vSphere Client 1457
Set Up Your System to Use Custom Certificates 1457
Managing Certificates with the vSphere Certificate Manager Utility 1460
Certificate Manager Options and the Workflows in This Document 1461
Regenerate a New VMCA Root Certificate and Replace All Certificates 1462
Make VMCA an Intermediate Certificate Authority (Certificate Manager) 1463
Replace All Certificates with Custom Certificate (Certificate Manager) 1466
Revert Last Performed Operation by Republishing Old Certificates 1469

Reset All Certificates Using the Certificate Manager 1469
Manual Certificate Replacement 1469
Understanding Stopping and Starting of Services 1469
Replace Existing VMCA-Signed Certificates with New VMCA-Signed Certificates 1470
Use VMCA as an Intermediate Certificate Authority 1476
Use Custom Certificates with vSphere 1483
Managing Services and Certificates with CLI Commands 1486
Required Privileges for Running CLIs 1486
Changing the certool Configuration Options 1487
certool Initialization Commands Reference 1488
certool Management Commands Reference 1490
vecs-cli Command Reference 1493
dir-cli Command Reference 1497
vSphere Authentication with vCenter Single Sign-On 1503
How vCenter Single Sign-On Protects Your Environment 1504
Understanding vCenter Server Identity Provider Federation 1506
How vCenter Server Identity Provider Federation Works 1506
vCenter Server Identity Provider Federation and Enhanced Linked Mode 1507
vCenter Server Identity Provider Federation Caveats and Interoperability 1508
vCenter Server Identity Provider Federation Life Cycle 1510
Configuring vCenter Server Identity Provider Federation 1510
vCenter Server Identity Provider Federation Configuration Process Flow 1510
Use the Trusted Root Certificates Store Instead of the JRE truststore 1512
Configure vCenter Server Identity Provider Federation for AD FS 1512
Understanding vCenter Single Sign-On 1515
vCenter Single Sign-On Components 1515
Using vCenter Single Sign-On with vSphere 1516
Groups in the vCenter Single Sign-On Domain 1516
Configuring vCenter Single Sign-On Identity Sources 1518
Identity Sources for vCenter Server with vCenter Single Sign-On 1518
Set the Default Domain for vCenter Single Sign-On 1519
Add or Edit a vCenter Single Sign-On Identity Source 1519
Use vCenter Single Sign-On with Windows Session Authentication 1523
Managing the vCenter Server Security Token Service 1524
Refresh a vCenter Server STS Certificate Using the vSphere Client 1524
Import and Replace a vCenter Server STS Certificate Using the vSphere Client 1526
Replace a vCenter Server STS Certificate Using the Command Line 1526
View the Active vCenter Server STS Signing Certificate Chain 1527
Determine the Expiration Date of an LDAPS SSL Certificate 1528
Managing vCenter Single Sign-On Policies 1528

Edit the vCenter Single Sign-On Password Policy....1528
Edit the vCenter Single Sign-On Lockout Policy....1530
Edit the vCenter Single Sign-On Token Policy....1530
Edit Password Expiration Notification for Active Directory (Integrated Windows Authentication) Users....1531
Managing vCenter Single Sign-On Users and Groups....1532
Add vCenter Single Sign-On Users....1532
Disable and Enable vCenter Single Sign-On Users....1533
Delete a vCenter Single Sign-On User....1533
Edit a vCenter Single Sign-On User....1534
Add a vCenter Single Sign-On Group....1534
Add Members to a vCenter Single Sign-On Group....1535
Remove Members from a vCenter Single Sign-On Group....1536
Change Your vCenter Single Sign-On Password....1536
Understanding Other Authentication Options....1537
Smart Card Authentication Login....1538
Configuring and Using Smart Card Authentication....1538
Set Up RSA SecurID Authentication....1544
Managing the Login Message to the vSphere Client Login Page....1545
Manage the Login Message to the vSphere Client Login Page....1546
vCenter Single Sign-On Security Best Practices....1546
Troubleshooting Authentication....1547
Determining the Cause of a Lookup Service Error....1547
Unable to Log In Using Active Directory Domain Authentication....1548
vCenter Server Login Fails Because the User Account Is Locked....1549
VMware Directory Service Replication Can Take a Long Time....1549
Export a vCenter Server Support Bundle....1549
Authentication Services Logs Reference....1550
Managing Host and Cluster Lifecycle....1551
Updated Information....1551
About vSphere Lifecycle Manager....1552
The vSphere Lifecycle Manager User Interface in the vSphere Client....1553
Bulletins, Components, Add-Ons, and ESXi Base Images....1555
vSphere Lifecycle Manager Baselines and Images....1557
System Requirements for Using vSphere Lifecycle Manager....1561
Privileges for Using vSphere Lifecycle Manager Images and Baselines....1562
Working with the vSphere Lifecycle Manager Depot....1564
Online and Offline Depots....1565
vSphere Lifecycle Manager Download Sources....1567
Browsing the vSphere Lifecycle Manager Depot....1568
Import Updates to the vSphere Lifecycle Manager Depot....1569

Import an ISO Image to the vSphere Lifecycle Manager Depot ... 1570
Delete an ISO Image from the vSphere Lifecycle Manager Depot ... 1571
Synchronize the vSphere Lifecycle Manager Depot ... 1571
Configuring the vSphere Lifecycle Manager Download Sources ... 1572
Configure vSphere Lifecycle Manager to Use a Shared Repository as a Download Source ... 1573
Configure vSphere Lifecycle Manager to Use the Internet as a Download Source ... 1574
Add a New Download Source ... 1575
Modify a Download Source ... 1576
Configure the vSphere Lifecycle Manager Automatic Download Task ... 1576
Run the VMware vSphere vSphere Lifecycle Manager Update Download Task ... 1577
Configuring the vSphere Lifecycle Manager Remediation Settings ... 1577
Cluster Settings and Host Remediation ... 1578
Configure Remediation Settings for vSphere Lifecycle Manager Images ... 1579
Configure Remediation Settings for vSphere Lifecycle Manager Baselines ... 1581
Configuring vSphere Lifecycle Manager for Fast Upgrades ... 1583
Creating vSphere Lifecycle Manager Clusters ... 1585
Create a Cluster That Uses a Single Image by Composing an Image Manually ... 1586
Create a Cluster That Uses a Single Image by Importing an Image from a Host ... 1587
Add Hosts to a Cluster that Uses a Single Image ... 1588
Using vSphere Lifecycle Manager Baselines and Baseline Groups ... 1592
Creating and Working with Baselines and Baseline Groups ... 1592
Baseline Types by Content ... 1594
Create a Fixed Patch Baseline ... 1595
Create a Dynamic Patch Baseline ... 1596
Create a Host Extension Baseline ... 1596
Create a Host Upgrade Baseline ... 1597
Create a Host Baseline Group ... 1598
Edit a Patch Baseline ... 1599
Edit a Host Extension Baseline ... 1599
Edit a Host Upgrade Baseline ... 1600
Edit a Baseline Group ... 1600
Add or Remove a Single Update from a Custom Baseline ... 1601
Duplicate Baselines and Baseline Groups ... 1601
Delete Baselines and Baseline Groups ... 1602
Attaching Baselines and Baseline Groups to vSphere Objects ... 1602
Attach Baselines and Baseline Groups to Objects ... 1602
Detach Baselines and Baseline Groups from Objects ... 1603
Checking Compliance Against vSphere Lifecycle Manager Baselines and Baseline Groups ... 1603
Initiate a Compliance Check for ESXi Hosts Manually ... 1604
Schedule Regular Compliance Checks for ESXi Hosts ... 1604

Host Upgrade Compliance Messages....1605
Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present....1607
Viewing Compliance Information About ESXi Hosts and Updates....1608
Staging Patches and Extensions to ESXi Hosts....1615
Stage Patches and Extensions to ESXi Hosts....1616
Remediating ESXi Hosts Against vSphere Lifecycle Manager Baselines and Baseline Groups....1616
Understanding the Remediation Operation....1618
Types of Host Remediation....1618
Remediating Hosts in a Cluster....1620
Remediating Hosts That Contain Third-Party Software....1620
Remediating ESXi 6.5 or ESXi6.7 Hosts Against an ESXi7.0 Image....1621
Remediation Pre-Check Report....1622
Generate a Pre-Remediation Check Report....1624
Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines....1624
Using vSphere Lifecycle Manager to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch....1626
Using vSphere Lifecycle Manager Images....1627
Working with Images....1628
Setting Up an Image....1628
Viewing Image Details....1629
Editing Images....1629
Reusing Existing Images....1631
Checking Compliance Against a Single Image....1634
Compliance States....1634
Check Cluster Compliance Against an Image....1635
View Host Compliance Information....1635
Run a Remediation Pre-Check for a Cluster....1636
Run a Remediation Pre-Check for a Single Host....1636
Remediating a Cluster Against a Single Image....1637
Edit the Remediation Settings for a Cluster....1638
Remediate a Cluster Against a Single Image....1640
Remediate a Single Host Against an Image....1640
View Last Remediation or Remediation Pre-Check Results for a Cluster that Uses a Single Image....1641
Manage Depot Overrides for a Cluster....1641
Recommended Images....1642
Check for Recommended Images....1643
Use a Recommended Image....1644
Switching from Using Baselines to Using Images....1645
Cluster Eligibility to Use vSphere Lifecycle Manager Images....1645
Set Up a New Image....1646

Import an Existing Image ... 1649
Firmware Updates ... 1650
Deploying Hardware Support Managers ... 1650
Use an Image for Firmware Updates ... 1651
Hardware Compatibility Checks ... 1652
Cluster-Level Hardware Compatibility Checks ... 1653
Host-Level Hardware Compatibility Checks ... 1658
vSphere Lifecycle Manager Images and Other VMware Products and Solutions ... 1661
vSAN Clusters and vSphere Lifecycle Manager ... 1661
Remediation Specifics of vSAN Clusters ... 1662
Updating Firmware in vSAN Clusters ... 1663
Using vSphere Lifecycle Manager Images to Remediate vSAN Stretched Clusters ... 1664
Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains ... 1665
About Recommendation Baseline Groups ... 1666
vSphere Lifecycle Manager and vSphere with Tanzu ... 1667
vSphere Lifecycle Manager and vSphere with Tanzu with vSphere Networking ... 1667
vSphere Lifecycle Manager and vSphere with Tanzu with NSX-T Data Center Networking ... 1669
vSphere Lifecycle Manager and VMware NSX-T Data Center™ ... 1670
Using vSphere Lifecycle Manager Baselines to Upgrade ESXi Hosts in an Environment With VMware NSX-T Data Center™ 3.0 ... 1670
Using vSphere Lifecycle Manager Images in an Environment With VMware NSX-T Data Center™ 3.1 ... 1671
Backup and Restore Scenarios When Using vSphere Lifecycle Manager ... 1672
Upgrading Virtual Machines with vSphere Lifecycle Manager ... 1673
Configure Virtual Machine Rollback Settings ... 1673
Checking the Status of Virtual Machines ... 1674
Check the Status of an Individual Virtual Machine ... 1675
Check the Status of the Virtual Machines in a Container Object ... 1675
The VMware Tools Status ... 1675
Upgrading Virtual Machines ... 1676
Upgrade the VM Hardware Compatibility of Virtual Machines ... 1677
Upgrade the VMware Tools Version of Virtual Machines ... 1678
Automatically Upgrade VMware Tools on Reboot ... 1679
Installing, Setting Up, and Using Update Manager Download Service ... 1679
Compatibility Between UMDS and vSphere Lifecycle Manager ... 1680
Installing UMDS ... 1680
Supported Linux-Based Operating Systems for Installing UMDS ... 1680
Install UMDS on a Linux OS ... 1681
Uninstall UMDS from a Linux OS ... 1681
Setting Up and Using UMDS ... 1682
Set Up the Data to Download with UMDS ... 1682

Change the UMDS Patch Repository Location....1682
Configure URL Addresses for Hosts....1683
Download the Specified Data Using UMDS....1683
Export the Downloaded Data....1684
vCenter Server Configuration....1685
About vCenter Server Configuration....1685
vCenter Server Configuration Overview....1685
What Happened to the Platform Services Controller....1686
Using the vCenter Server Management Interface to Configure vCenter Server....1686
Log In to the vCenter Server Management Interface....1687
View vCenter ServerHealth Status....1687
Reboot or Shut Down vCenter Server....1688
Create a Support Bundle....1688
Monitor CPU and Memory Use....1688
Monitor Disk Use....1688
Monitor Network Use....1688
Monitor Database Use....1689
Enable or Disable SSH and Bash Shell Access....1689
Configure the DNS, IP Address, and Proxy Settings....1690
Reconfigure the Primary Network Identifier....1691
Edit the Firewall Settings....1692
Configure the System Time Zone and Time Synchronization Settings....1693
Start, Stop, and Restart Services....1693
Configure Update Settings....1693
Change the Password and Password Expiration Settings of the Root User....1694
Forward vCenter Server Log Files to Remote Syslog Server....1694
Configure and Schedule Backups....1695
Using the vSphere Client to Configure vCenter Server....1695
Configuring vCenter Server....1696
Configure License Settings for vCenter Server....1696
Configuring Statistics Settings....1696
Configure Runtime Settings for vCenter Server....1698
Configure User Directory Settings....1699
Configure Mail Sender Settings....1700
Configure SNMP Settings....1701
View Port Settings....1701
Configure Timeout Settings....1702
Configure Logging Options....1702
Configure Database Settings....1703
Verifying SSL Certificates for Legacy Hosts....1704

Configure Advanced Settings ... 1704
Send a Message to Other Logged In Users ... 1705
Join or Leave an Active Directory Domain ... 1705
Add a User to the SystemConfiguration.BashShellAdministrators Group ... 1707
Reboot a Node ... 1707
View the Health Status of Nodes ... 1708
Export a Support Bundle ... 1708
Using the Appliance Shell to Configure vCenter Server ... 1709
Access the Appliance Shell ... 1709
Enable and Access the Bash Shell from the Appliance Shell ... 1709
Keyboard Shortcuts for Editing Commands ... 1709
Get Help About the Plug-Ins and API Commands in the Appliance ... 1711
Plug-Ins in the vCenter Server Shell ... 1711
Browse the Log Files By Using the showlog Plug-In ... 1712
API Commands in the Appliance Shell ... 1712
Configuring SNMP for vCenter Server ... 1717
Configure the SNMP Agent for Polling ... 1717
Configure vCenter Serverfor SNMP v1 and v2c ... 1717
Configure vCenter Server for SNMP v3 ... 1718
Configure the SNMP Agent to Filter Notifications ... 1721
Configure SNMP Management Client Software ... 1721
Reset SNMP Settings to Factory Defaults ... 1722
Configuring Time Synchronization Settings in vCenter Server ... 1722
Use VMware Tools Time Synchronization ... 1723
Add or Replace NTP Servers in the vCenter Server Configuration ... 1723
Synchronize the Time in vCenter Server with an NTP Server ... 1723
Managing Local User Accounts in vCenter Server ... 1724
User Roles in vCenter Server ... 1724
Get a List of the Local User Accounts in vCenter Server ... 1724
Create a Local User Account in vCenter Server ... 1724
Update the Password of a Local User in vCenter Server ... 1725
Update a Local User Account in vCenter Server ... 1725
Delete a Local User Account in vCenter Server ... 1726
Monitor Health Status and Statistics in vCenter Server ... 1726
Using the vimtop Plug-In to Monitor the Resource Use of Services ... 1726
Monitor Services By Using vimtop in Interactive Mode ... 1727
Interactive Mode Command-Line Options ... 1727
Interactive Mode Single-Key Commands for vimtop ... 1727
Using the Direct Console User Interface to Configure vCenter Server ... 1729
Log In to the Direct Console User Interface ... 1729

Change the Password of the Root User ... 1729
Configure the Management Network of vCenter Server ... 1730
Restart the Management Network of vCenter Server ... 1731
Enable Access to the Bash Shell ... 1731
Access the Bash Shell for Troubleshooting ... 1731
Export a vCenter Server Support Bundle for Troubleshooting ... 1731
vCenter Server and Host Management ... 1733
Updated Information ... 1733
vSphere Concepts and Features ... 1734
Virtualization Basics ... 1734
Physical Topology of vSphere Data Center ... 1735
vSphere Software Components ... 1735
vSphere Cluster Services ... 1738
Monitoring vSphere Cluster Services ... 1739
Maintaining Health of vSphere Cluster Services ... 1740
Client Interfaces for vSphere ... 1741
vSphere Managed Inventory Objects ... 1741
Optional vCenter Server Components ... 1743
vCenter Server Plug-Ins ... 1744
Using the vSphere Client ... 1744
Log In to vCenter Server by Using the vSphere Client ... 1745
Manage the Login Message to the vSphere Client Login Page ... 1745
Navigate the vSphere Inventory by Using the Global Inventory Lists Navigator ... 1746
Manage Client Plug-Ins ... 1747
Monitor Client Plug-Ins ... 1747
Refresh Data ... 1747
Searching the Inventory ... 1747
Perform a Quick Search ... 1748
Save a Search ... 1748
Manage a Saved Search ... 1749
Sort the vSphere Client Inventory ... 1749
Drag Objects ... 1750
Keyboard Shortcuts ... 1750
Inventory Keyboard Shortcuts ... 1750
Export Lists ... 1751
Configure the vSphere Client Timeout Value ... 1751
Attach File to Service Request ... 1752
Provide Feedback with the vSphere Client ... 1752
Start, Stop, and Restart Services ... 1752
Submit Suggestions for New Features and Feature Requests Through the vSphere Ideas Portal ... 1753

Using Enhanced Linked Mode **1753**
Configuring Customer Experience Improvement Program **1753**
VMware Customer Experience Improvement Program 1753
Join or Leave Customer Experience Improvement Program in vSphere Client 1754
Organizing Your Inventory **1754**
Create a Data Center 1755
Create a Folder 1755
Add a Host to a Folder or a Data Center 1755
Creating and Configuring Clusters 1756
Create a Cluster 1757
Add a Host to a Cluster 1758
Configure a Cluster 1760
Extend a Cluster 1761
Extend a Cluster Without Host Networking Configuration 1761
Use Quickstart to Extend a Cluster with Host Networking Configuration 1762
vSphere Tags and Attributes **1764**
Create, Edit, or Delete a Tag Category 1764
Create a Tag 1765
Edit or Delete a Tag 1766
Assign or Remove a Tag 1766
Add Permissions for Tags and Tag Categories 1766
vSphere Tagging Best Practices 1767
Custom Attributes 1767
Add and Edit Custom Attributes 1768
Working with Tasks **1768**
View Tasks 1768
Cancel a Task 1769
Export Tasks 1770
Schedule Tasks 1770
Create a Scheduled Task 1771
Change or Reschedule a Task 1772
Remove a Scheduled Task 1772
Configuring Hosts in vCenter Server **1772**
Host Configuration 1773
Configure the Boot Device on an ESXi Host 1773
Configure Agent VM Settings 1773
Set Advanced Host Attributes 1774
Synchronizing Clocks on the vSphere Network 1774
Editing the Time Configuration Settings of a Host 1775
Managing Hosts with vCenter Server **1778**

Disconnecting and Reconnecting a Host....1778
Disconnect a Managed Host....1778
Reconnect a Managed Host....1779
Reconnecting Hosts After Changes to the vCenter Server SSL Certificate....1779
Relocate a Host....1779
Remove a Managed Host from vCenter Server....1779
Reboot or Shut Down an ESXi Host....1780
Verifying SSL Certificates for Legacy Hosts....1781
License and Subscription Management....1781
Licensing and Subscription Terminology and Definitions....1781
The License Service in vSphere 7.0....1782
Licensing for Environments with vCenter Server Systems 6.0 and Later, and 5.5....1783
Licensing and Subscription for Products in vSphere....1783
Licensing for ESXi Hosts....1783
Licensing for vCenter Server....1784
Licensing for Clusters with vSAN Enabled....1785
Licensing for vSphere with Tanzu....1786
vSphere+ and vSAN+ Subscriptions....1787
Subscription Information for Your vCenter Server....1788
View Subscription Information About Your vCenter Server....1788
View Subscription Information About a vSAN Cluster....1788
Managing Licenses....1789
Create New Licenses....1789
Configuring License Settings for Assets in the vSphere Client....1789
Set Assets to Evaluation Mode....1793
Rename a License....1793
Remove Licenses....1794
Viewing Licensing Information....1794
View Licensing Information About the vSphere Environment....1794
View Available Licenses and Features About a Product....1797
View the Features That an Asset Can Use....1797
View the License Key of the License....1797
View the Licensed Features for an Asset....1797
Export Licensing Information in the vSphere Environment....1798
vCenter Server Domain Repoint License Considerations....1798
Migrating Virtual Machines....1799
Cold Migration....1800
Migration with vMotion....1801
Host Configuration for vMotion....1802
Encrypted vSphere vMotion....1804

Virtual Machine Conditions and Limitations for vMotion ... 1807
Migration with vMotion in Environments Without Shared Storage ... 1809
Migration Between vCenter Server Systems ... 1810
Migration with Storage vMotion ... 1820
Storage vMotion Requirements and Limitations ... 1820
CPU Compatibility and EVC ... 1820
CPU Compatibility Scenarios ... 1821
CPU Families and Feature Sets ... 1822
About Enhanced vMotion Compatibility ... 1822
EVC Requirements for Hosts ... 1822
Enable EVC on an Existing Cluster ... 1823
Change the EVC Mode for a Cluster ... 1823
Determine the EVC Mode of a Virtual Machine ... 1825
Determine the EVC Mode that a Host Supports ... 1827
Prepare Clusters for AMD Processors Without 3DNow! ... 1827
CPU Compatibility Masks ... 1828
View Feature Capabilities Details for an EVC Cluster ... 1828
Migrate a Powered Off or Suspended Virtual Machine ... 1828
Migrate a Virtual Machine to a New Compute Resource ... 1831
Migrate a Virtual Machine to a New Compute Resource and Storage ... 1834
Migrate a Virtual Machine to New Storage ... 1840
Place vMotion Traffic on the vMotion TCP/IP Stack of an Host ... 1844
Place Traffic for Cold Migration on the Provisioning TCP/IP Stack ... 1849
Limits on Simultaneous Migrations ... 1855
Migration Compatibility Checks ... 1856
Working with the Developer Center ... 1857
Using the API Explorer ... 1857
Retrieve APIs Using API Explorer ... 1857
Using Code Capture ... 1857
Record Actions Using Code Capture ... 1857
Automating Management Tasks by Using vRealize Orchestrator ... 1858
Concepts of Workflows ... 1858
Performing Administration Tasks on the vSphere Objects ... 1859
Configure the Default vRealize Orchestrator ... 1859
Managing Associations of Workflows with vSphere Inventory Objects ... 1860
Associate Workflows with vSphere Inventory Object Types ... 1860
Edit the Associations of Workflows with vSphere Objects ... 1861
Export the Associations of Workflows with vSphere Objects ... 1861
Import the Association of Workflows with vSphere Objects ... 1862
Working with Workflows ... 1862

Run Workflows on vSphere Inventory Objects....1862
View Information About Workflow Runs....1863
View Information About the Runs of a Specific Workflow....1863
View Workflows That Are Waiting for User Interaction....1864
Searching for Workflows....1864
Scheduling Workflows....1865
Workflows for Managing Inventory Objects....1867
Cluster and Compute Resource Workflows....1868
Guest Operation Files Workflows....1868
Guest Operation Processes Workflows....1868
Custom Attributes Workflows....1869
Data Center Workflows....1869
Datastore and Files Workflows....1869
Data Center Folder Management Workflows....1869
Host Folder Management Workflows....1870
Virtual Machine Folder Management Workflows....1870
Basic Host Management Workflows....1870
Host Power Management Workflows....1870
Host Registration Management Workflows....1870
Networking Workflows....1871
Distributed Virtual Port Group Workflows....1871
Distributed Virtual Switch Workflows....1871
Standard Virtual Switch Workflows....1872
Resource Pool Workflows....1872
Storage Workflows....1872
Storage DRS Workflows....1873
Basic Virtual Machine Management Workflows....1873
Clone Workflows....1874
Linked Clone Workflows....1874
Linux Customization Clone Workflows....1875
Tools Clone Workflows....1875
Windows Customization Clone Workflows....1875
Device Management Workflows....1876
Move and Migrate Workflows....1876
Other Workflows....1877
Power Management Workflows....1878
Snapshot Workflows....1878
VMware Tools Workflows....1878
About Headless Systems....1879
How to Detect a Headless System....1879

About Serial Mode Dynamic Switching....1879
ESXi Serial Port Modes....1879
Dynamic Switching Keystrokes....1880
Serial Port Dynamic Switching Using the CLI....1880
Controlling the Serial DCUI....1880
Troubleshooting Overview....1881
Troubleshooting vCenter Server....1881
Guidelines for Troubleshooting....1881
Identifying Symptoms....1881
Defining the Problem Space....1882
Testing Possible Solutions....1882
Troubleshooting with vCenter Server Logs....1882
Troubleshooting vCenter Server and ESXi Host Certificates....1883
New vCenter Server Certificate Does Not Appear to Load....1884
vCenter Server Cannot Connect to Managed Hosts....1884
Troubleshooting Hosts....1884
Troubleshooting vSphere HA Host States....1884
Authentication Token Manipulation Error....1887
Unable to Download VIBs When Using vCenter Server Reverse Proxy....1888
Troubleshooting Licensing....1889
Troubleshooting Host Licensing....1889
Unable to Power On a Virtual Machine....1890
Unable to Configure or Use a Feature....1890
vSphere Virtual Machine Administration Guide....1891
Introduction to VMware vSphere Virtual Machines....1891
Virtual Machine Files....1891
Virtual Machines and the Virtual Infrastructure....1892
Virtual Machine Lifecycle....1892
Virtual Machine Components....1893
Virtual Machine Hardware Available to vSphere Virtual Machines....1894
Virtual Machine Options....1896
ThevSphere Client....1897
Where to Go From Here....1897
Deploying Virtual Machines....1897
Create a Virtual Machine with the New Virtual Machine Wizard....1897
Clone a Virtual Machine to a Template....1899
Deploy a Virtual Machine from a Template....1902
Clone an Existing Virtual Machine....1904
Cloning a Virtual Machine with Instant Clone....1907
Clone a Template to a Template....1908

Convert a Template to a Virtual Machine....1910
Deploying OVF and OVA Templates....1910
OVF and OVA File Formats and Templates....1910
Deploy an OVF or OVA Template....1911
Export an OVF Template....1912
Browse VMware Virtual Appliance Marketplace....1913
Using Content Libraries....1913
Hierarchical Inheritance of Permissions for Content Libraries....1914
Content Library Administrator Role....1916
Create a Library....1916
Edit a Content Library....1918
Configure Advanced Content Library Settings....1919
Managing a Publisher Local Library....1920
Create a Subscription for a Local Library....1921
Publish the Contents of a Library to a Subscriber....1923
Publish a Single Template to a Subscription....1923
Delete a Subscription....1924
Managing a Subscribed Library....1924
Synchronize a Subscribed Content Library....1925
Synchronize a Library Item in a Subscribed Library....1926
Populating Libraries with Content....1926
Import Items to a Content Library....1926
Clone a vApp to a Template in a Content Library....1927
Clone a Virtual Machine or a Virtual Machine Template to a Template in a Content Library....1928
Working with Items in a Library....1929
Update a Content Library Item....1929
Export an Item from a Content Library to Your Local Computer....1929
Clone Library Items from One Library to Another Library....1930
Edit a Content Library Item....1930
Delete a Content Library Item....1931
Creating Virtual Machines and vApps from Templates in a Content Library....1931
Deploy a Virtual Machine from an OVF Template in a Content Library....1931
Deploy a Virtual Machine from a VM Template in a Content Library....1933
Create New vApp From a Template in a Content Library....1936
Managing VM Templates....1936
Templates in Content Libraries....1936
Check Out a Virtual Machine from a Template....1938
Check In a Virtual Machine to a Template....1939
Discard a Checked Out Virtual Machine....1939
Revert to a Previous Version of a Template....1940

Delete a Previous Version of a VM Template ... 1941
Configuring Virtual Machine Hardware ... 1941
Virtual Machine Compatibility ... 1941
Set the Default Compatibility for Virtual Machine Creation ... 1943
Schedule a Compatibility Upgrade for a Single Virtual Machine ... 1944
Change the Default Virtual Machine Compatibility Setting ... 1944
Hardware Features Available with Virtual Machine Compatibility Settings ... 1945
Virtual CPU Configuration ... 1948
Virtual CPU Limitations ... 1949
Configuring Multicore Virtual CPUs ... 1949
Enable CPU Hot Add ... 1950
Change the Number of Virtual CPUs ... 1950
Expose VMware Hardware Assisted Virtualization ... 1951
Activate Virtual CPU Performance Counters ... 1951
Configure Processor Scheduling Affinity ... 1952
Activate IO/MMU Virtualization Settings ... 1952
Virtual Memory Configuration ... 1953
Change the Memory Configuration ... 1953
Allocate Memory Resources ... 1954
Managing Persistent Memory ... 1955
Change Memory Hot Add Settings ... 1957
Virtual Disk Configuration ... 1958
About Virtual Disk Provisioning Policies ... 1958
Large Capacity Virtual Disk Conditions and Limitations ... 1959
Change the Virtual Disk Configuration ... 1959
Use Disk Shares to Prioritize Virtual Machines ... 1960
Determine the Virtual Disk Format and Convert a Virtual Disk from Thin Provision to a Thick Provision Format ... 1961
Add a Hard Disk to a Virtual Machine ... 1962
SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility ... 1966
Add a SATA Controller ... 1968
Add a SCSI Controller to a Virtual Machine ... 1969
Add a Paravirtualized SCSI Adapter ... 1969
Add an NVMe Controller ... 1970
Change the SCSI Controller Configuration ... 1970
Virtual Machine Network Configuration ... 1971
Network Adapter Basics ... 1971
Network Adapters and Legacy Virtual Machines ... 1972
Change the Virtual Machine Network Adapter Configuration ... 1973
Add a Network Adapter to a Virtual Machine ... 1973

Parallel and Serial Port Configuration....1974
Other Virtual Machine Device Configuration.... 1980
Change the CD/DVD Drive Configuration.... 1980
How do I Add or Modify a Virtual Machine CD or DVD Drive....1982
Add a PCI Device to a Virtual Machine.... 1984
Configuring 3D Graphics.... 1986
Using a Virtual Watchdog Timer....1988
Add a Precision Clock Device to a Virtual Machine....1989
Securing Virtual Machines with Intel Software Guard Extensions....1990
Enable vSGX on a Virtual Machine....1990
Remove vSGX from a Virtual Machine.... 1991
USB Configuration from an ESXi Host to a Virtual Machine.... 1992
USB Autoconnect Feature....1993
vSphere Features Available with USB Passthrough.... 1994
Conditions and Limitations When Configuring USB Devices for vMotion.... 1994
Avoiding Data Loss with USB Devices.... 1994
Connecting USB Devices to an ESXi Host....1995
Add USB Devices to an ESXi Host....1996
Add a USB Controller to a Virtual Machine.... 1996
Add USB Devices from an ESXi Host to a Virtual Machine.... 1997
Remove USB Devices That Are Connected Through an ESXi Host.... 1998
Remove USB Devices from an ESXi Host....1998
USB Configuration from a Client Computer to a Virtual Machine.... 1998
Connecting USB Devices to a Client Computer.... 1999
Connect a USB Device to a Client Computer....2000
Add a USB Controller to a Virtual Machine....2001
Add USB Devices from a Client Computer to a Virtual Machine....2002
Remove USB Devices That Are Connected Through a Client Computer....2002
Remove a USB Controller from a Virtual Machine.... 2002
Add a Shared Smart Card Reader to Virtual Machines....2003
Securing Virtual Machines with Virtual Trusted Platform Module....2003
Virtual Trusted Platform Module Overview....2004
Create a Virtual Machine with a Virtual Trusted Platform Module.... 2005
Enable Virtual Trusted Platform Module for an Existing Virtual Machine....2005
Remove Virtual Trusted Platform Module from a Virtual Machine.... 2006
Identify Virtual Trusted Platform Module Enabled Virtual Machines.... 2007
Securing Virtual Machines with AMD Secure Encrypted Virtualization-Encrypted State....2007
vSphere and AMD Secure Encrypted Virtualization-Encrypted State....2007
Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine with the vSphere Client... 2008

Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine with the vSphere Client....2009
Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine....2010
Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine....2010
Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine with the vSphere Client....2011
Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine....2011
Configuring Virtual Machine Options....2012
Configure General Virtual Machine Options....2012
General Virtual Machine Options....2013
Change the Virtual Machine Name....2013
View the Virtual Machine Configuration and Working File Location....2013
Change the Configured Guest Operating System....2014
Configuring User Mappings on Guest Operating Systems....2014
View Existing SSO User Mappings....2015
Add SSO users to Guest Operating Systems....2015
Remove SSO Users from Guest Operating Systems....2015
VMware Remote Console Options....2015
Change the Virtual Machine Console Options for Remote Users....2015
Configure Virtual Machine Encryption Options....2016
Encrypt an Existing Virtual Machine or Virtual Disk....2016
Decrypt an Encrypted Virtual Machine or Virtual Disk....2017
Clone an Encrypted Virtual Machine....2018
Virtual Machine Power Management Options....2019
Manage Power Management Settings for a Virtual Machine....2019
Configuring VMware Tools Options....2019
Configure the Virtual Machine Power States....2019
Synchronize the Time of a Virtual Machine Guest Operating System with the Host....2020
Virtualization Based Security....2021
Enable Virtualization-based Security on an Existing Virtual Machine....2022
Enable Virtualization-based Security on the Guest Operating System....2022
Deactivate Virtualization-based Security....2023
Identify VBS-Enabled Virtual Machines....2023
Configure Virtual Machine Boot Options....2023
Activate or Deactivate UEFI Secure Boot for a Virtual Machine....2023
Delay the Boot Sequence....2025
Configuring Virtual Machine Advanced Options....2025
Deactivating Virtual Machine Acceleration....2025
Enable Virtual Machine Logging....2025
Configure Virtual Machine Debugging and Statistics....2026

Change the Swap File Location....2026
Edit Configuration File Parameters....2027
Configure Fibre Channel NPIV Settings....2027
Managing Multi-Tiered Applications with vSphere vApp....2028
Create a vApp....2028
Perform vApp Power Operations....2029
Create or Add an Object to a vApp....2030
Clone a vApp....2030
Edit vApp Notes....2031
Configure vApp Properties....2031
Edit vApp Settings....2032
Configure vApp CPU and Memory Resources....2032
Configure vApp IP Allocation Policy....2033
Configure vApp Startup and Shutdown Options....2033
Configure vApp Product Properties....2034
View vApp License Agreements....2034
Add a Network Protocol Profile....2034
Assign a Port Group or Network to a Network Protocol Profile....2036
Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp....2037
Virtual Machine vApp Options....2038
Activate vApp Options for a Virtual Machine....2038
Edit Application Properties and OVF Deployment Options for a Virtual Machine....2038
OVF Authoring Options for a Virtual Machine....2039
Monitoring Solutions with the vCenter Solutions Manager....2042
View Solutions....2042
vSphere ESX Agent Manager....2043
Monitor ESX Agent Health Status....2043
Resolve Agency Issues....2043
Managing Virtual Machines....2044
Installing a Guest Operating System....2044
Using PXE with Virtual Machines....2044
Install a Guest Operating System from Media....2044
Upload ISO Image Installation Media for a Guest Operating System....2045
Customizing Guest Operating Systems....2046
Guest Operating System Customization Requirements....2046
Create a vCenter Server Application to Generate Computer Names and IP Addresses....2046
Customize Windows During Cloning or Deployment....2047
Customize Linux During Cloning or Deployment....2048
Apply a Customization Specification to an Existing Virtual Machine....2049
Creating and Managing Customization Specifications....2049

Managing Power States of a Virtual Machine 2056
Edit Virtual Machine Startup and Shutdown Settings 2057
Using a Virtual Machine Console 2058
Install the VMware Remote Console Application 2058
Start the VMware Remote Console Application 2061
Open the Web Console 2061
Manage the VMware Remote Console Proxy Configuration 2062
Answer Virtual Machine Questions 2064
Removing and Reregistering VMs and VM Templates 2065
Adding Existing Virtual Machines to vCenter Server 2065
Remove VMs or VM Templates from vCenter Server or from the Datastore 2065
Register a VM or VM Template with vCenter Server 2066
Managing Virtual Machine Templates 2066
Change the Template Name 2066
Deleting Templates 2066
Using Snapshots To Manage Virtual Machines 2067
Snapshot Files 2069
Snapshot Limitations 2070
Managing Snapshots 2070
Taking Snapshots of a Virtual Machine 2071
Revert a Virtual Machine Snapshot 2073
Delete a Snapshot 2074
Consolidate Snapshots 2075
Enhanced vMotion Compatibility as a Virtual Machine Attribute 2076
Configure the EVC Mode of a Virtual Machine 2077
Determine the EVC Mode of a Virtual Machine 2079
Virtual Machine Storage DRS Rules 2080
Add a VMDK Affinity Rule 2081
Add a VMDK Anti-Affinity Rule 2082
Add a VM Anti-Affinity Rule 2082
Distributing Content with GuestStore 2083
Set the GuestStore Repository with ESXCLI 2085
Clear the GuestStore Repository Setting with ESXCLI 2085
Migrating Virtual Machines 2085
Virtual Machine Conditions and Limitations for vMotion 2087
Migrate a Powered Off or Suspended Virtual Machine 2087
Migrate a Virtual Machine to a New Compute Resource 2093
Migrate a Virtual Machine to New Storage 2096
Migrate a Virtual Machine to a New Compute Resource and Storage 2100
Upgrading Virtual Machines 2106

Downtime for Upgrading Virtual Machines 2107
Upgrade the Compatibility of a Virtual Machine Manually 2108
Schedule a Compatibility Upgrade for a Virtual Machine 2108
Required vCenter Server Privileges for Common Tasks 2109
Troubleshooting Overview 2112
Guidelines for Troubleshooting 2112
Identifying Symptoms 2112
Defining the Problem Space 2113
Testing Possible Solutions 2113
Troubleshooting with vCenter Server Logs 2113
Troubleshooting Virtual Machines 2114
Troubleshooting USB Passthrough Devices 2114
Error Message When You Try to Migrate Virtual Machine with USB Devices Attached 2115
Cannot Copy Data From an ESXi Host to a USB Device That Is Connected to the Host 2115
Recover Orphaned Virtual Machines 2115
vSphere Host Profiles 2117
Updated Information 2117
Introduction To vSphere Host Profiles 2117
Host Profiles Usage Model 2117
Reference Host Independence 2118
Reference Host Selection 2118
Using Host Profiles 2119
Access Host Profiles 2119
Create a Host Profile 2119
Attach or Detach Hosts and Clusters to a Host Profile 2120
Check Compliance 2120
Schedule Compliance Check 2120
Remediate a Host 2121
Edit a Host Profile 2122
Edit a Policy 2122
Disable Host Profile Component or Subprofile 2124
Duplicate a Host Profile 2125
Copy Settings from Host 2125
Host Profiles and vSphere Auto Deploy 2125
Import a Host Profile 2126
Export a Host Profile 2126
Copy Settings to Host Profile 2126
Configuring Host Profiles 2126
Host Customization 2126
Export Host Customizations 2130

Edit Host Customizations....2130
Configure Security Host Profile....2130
Configure Networking Host Profiles....2131
Recommended Host Profiles Upgrade Workflows....2132
vCenter Server Upgrade from 6.5 to 7.0 With Stateful ESXi Hosts Version 6.5 or Earlier....2133
Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi6.0 and 6.5 Hosts....2133
Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi 6.5 Hosts Only....2134
vCenter Server Upgrade from 6.7 to 7.0 With Stateful ESXi Hosts Version 6.7 or Earlier....2134
Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi6.0, 6.5, and 6.7 Hosts....2134
Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi 6.5 and 6.7 Hosts....2135
Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi6.7 Hosts Only....2136
vCenter Server Upgrade from 6.5 to 7.0 in an Environment with Stateless ESXi 6.5 Hosts Only....2136
vCenter Server Upgrade from 6.7 to 7.0 in an Environment With Stateless ESXi6.7 Hosts Only....2137
Using Host Profiles to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch....2138
Answer File Field and Host Profile Extraction....2139
Troubleshooting Host Profiles....2140
Host Customization Data Is Missing....2140
Reference Host is Unavailable....2140
Compliance Failures with Storage Host Profiles....2141
Compliance Failures with Serial Attached SCSI (SAS) Devices....2141
Compliance failures with SAN Boot LUN Devices....2141
Edit Settings for Host Profiles is Failing....2142
Host Profile without NFS Datastore....2142
Upgraded Host is Not Compliant with a Legacy Host Profile....2143
vSphere Networking....2144
Updated Information....2144
Introduction to vSphere Networking....2144
Networking Concepts Overview....2144
Network Services in ESXi....2146
VMware ESXi Dump Collector Support....2147
Setting Up Networking with vSphere Standard Switches....2147
vSphere Standard Switches....2147
Create a vSphere Standard Switch....2149
Port Group Configuration for Virtual Machines....2150
Add a Virtual Machine Port Group....2151
Edit a Standard Switch Port Group....2152
Remove a Port Group from a vSphere Standard Switch....2153
vSphere Standard Switch Properties....2153
Change the Size of the MTU on a vSphere Standard Switch....2154
Change the Speed of a Physical Adapter....2154

Add and Team Physical Adapters in a vSphere Standard Switch.... 2155
View the Topology Diagram of a vSphere Standard Switch.... 2155
Setting Up Networking with vSphere Distributed Switches.... 2156
vSphere Distributed Switch Architecture.... 2156
Create a vSphere Distributed Switch.... 2160
Upgrade a vSphere Distributed Switch to a Later Version.... 2162
Edit General and Advanced vSphere Distributed Switch Settings.... 2163
Managing Networking on Multiple Hosts on a vSphere Distributed Switch.... 2164
Tasks for Managing Host Networking on a vSphere Distributed Switch.... 2164
Add Hosts to a vSphere Distributed Switch.... 2165
Configure Physical Network Adapters on a vSphere Distributed Switch.... 2168
Migrate VMkernel Adapters to a vSphere Distributed Switch.... 2169
Create a VMkernel Adapter on a vSphere Distributed Switch.... 2170
Migrate Virtual Machine Networking to the vSphere Distributed Switch.... 2179
Remove Hosts from a vSphere Distributed Switch.... 2180
Managing Networking on Host Proxy Switches.... 2181
Migrate Network Adapters on a Host to a vSphere Distributed Switch.... 2181
Migrate a VMkernel Adapter on a Host to a vSphere Standard Switch.... 2182
Assign a Physical NIC of a Host to a vSphere Distributed Switch.... 2183
Remove a Physical NIC from a vSphere Distributed Switch.... 2183
Removing NICs from Active Virtual Machines.... 2183
Distributed Port Groups.... 2183
Add a Distributed Port Group.... 2184
Edit General Distributed Port Group Settings.... 2187
Remove a Distributed Port Group.... 2188
Working with Distributed Ports.... 2188
Monitor the State of Distributed Ports.... 2188
Configure Distributed Port Settings.... 2189
Configuring Virtual Machine Networking on a vSphere Distributed Switch.... 2189
Migrate Virtual Machines to or from a vSphere Distributed Switch.... 2189
Connect an Individual Virtual Machine to a Distributed Port Group.... 2190
Topology Diagrams of a vSphere Distributed Switch.... 2190
View the Topology of a vSphere Distributed Switch.... 2191
View the Topology of a Host Proxy Switch.... 2192
Setting Up VMkernel Networking.... 2192
VMkernel Networking Layer.... 2192
View Information About VMkernel Adapters on a Host.... 2194
Create a VMkernel Adapter on a vSphere Standard Switch.... 2195
Create a VMkernel Adapter on a Host Associated with a vSphere Distributed Switch.... 2208
Edit a VMkernel Adapter Configuration.... 2220

Overriding the Default Gateway of a VMkernel Adapter....2225
Configure the VMkernel Adapter Gateway by Using esxcli Commands....2225
Configure the resolv.conf File by Using esxcli Commands....2226
Configure the DNS Hosts File by Using ESXCLI Commands....2227
View TCP/IP Stack Configuration on a Host....2228
Change the Configuration of a TCP/IP Stack on a Host....2228
Explicit Congestion Notification....2229
Create a Custom TCP/IP Stack....2229
Remove a VMkernel Adapter....2230
LACP Support on a vSphere Distributed Switch....2230
Configure LACP Teaming and Failover for Distributed Port Groups....2232
Configure a Link Aggregation Group to Handle the Traffic for Distributed Port Groups....2233
Edit a Link Aggregation Group....2236
Limitations of the LACP Support on a vSphere Distributed Switch....2236
Backing Up and Restoring Networking Configurations....2237
Backing Up and Restoring a vSphere Distributed Switch Configuration....2237
Export vSphere Distributed Switch Configurations....2237
Import a vSphere Distributed Switch Configuration....2238
Restore a vSphere Distributed Switch Configuration....2238
Export, Import, and Restore vSphere Distributed Port Group Configurations....2238
Export vSphere Distributed Port Group Configurations....2239
Import a vSphere Distributed Port Group Configuration....2240
Restore a vSphere Distributed Port Group Configuration....2240
Rollback and Recovery of the Management Network....2240
vSphere Networking Rollback....2240
Disable Network Rollback....2241
Disable Network Rollback by Using the vCenter Server Configuration File....2242
Resolve Errors in the Management Network Configuration on a vSphere Distributed Switch....2242
Networking Policies....2243
Applying Networking Policies on a vSphere Standard or Distributed Switch....2243
Configure Overriding Networking Policies on Port Level....2244
Teaming and Failover Policy....2244
Load Balancing Algorithms Available for Virtual Switches....2246
Configure NIC Teaming, Failover, and Load Balancing on a vSphere Standard Switch or Standard Port Group....2250
Configure NIC Teaming, Failover, and Load Balancing on a Distributed Port Group or Distributed Port....2252
VLAN Policy....2254
Configure VLAN Tagging on a Distributed Port Group or Distributed Port....2254
Configure VLAN Tagging on an Uplink Port Group or Uplink Port....2255
Security Policy....2256

Configure the Security Policy for a vSphere Standard Switch or Standard Port Group....2256
Configure the Security Policy for a Distributed Port Group or Distributed Port....2257
Traffic Shaping Policy....2258
Configure Traffic Shaping for a vSphere Standard Switch or Standard Port Group....2259
Edit the Traffic Shaping Policy on a Distributed Port Group or Distributed Port....2260
Resource Allocation Policy....2261
Edit the Resource Allocation Policy on a Distributed Port Group....2261
Monitoring Policy....2261
Manage NetFlow Monitoring on a Distributed Port Group or Distributed Port....2261
Traffic Filtering and Marking Policy....2262
Traffic Filtering and Marking on a Distributed Port Group or Uplink Port Group....2262
Traffic Filtering and Marking on a Distributed Port or Uplink Port....2267
Qualifying Traffic for Filtering and Marking....2273
Manage Policies for Multiple Port Groups on a vSphere Distributed Switch....2277
Port Blocking Policies....2280
Edit the Port Blocking Policy for a Distributed Port Group....2280
Edit the Blocking Policy for a Distributed Port or Uplink Port....2280
MAC Learning Policy....2281
Isolating Network Traffic by Using VLANs....2281
VLAN Configuration....2281
Private VLANs....2282
Create a Private VLAN....2283
Remove a Primary Private VLAN....2283
Remove a Secondary Private VLAN....2283
Managing Network Resources....2284
DirectPath I/O....2284
Enable Passthrough for a Network Device on a Host....2284
Configure a PCI Device on a Virtual Machine....2285
Single Root I/O Virtualization (SR-IOV)....2285
SR-IOV Support....2286
SR-IOV Component Architecture and Interaction....2287
vSphere and Virtual Function Interaction....2289
DirectPath I/O vs SR-IOV....2290
Configure a Virtual Machine to Use SR-IOV....2290
Networking Options for the Traffic Related to an SR-IOV Enabled Virtual Machine....2291
Using an SR-IOV Physical Adapter to Handle Virtual Machine Traffic....2292
Enabling SR-IOV by Using Host Profiles or an ESXCLI Command....2293
Virtual Machine That Uses an SR-IOV Virtual Function Fails to Power On Because the Host Is Out of Interrupt Vectors....2294
Remote Direct Memory Access for Virtual Machines....2295

PVRDMA Support ... 2295
Configure an ESXi Host for PVRDMA ... 2296
Assign a PVRDMA Adapter to a Virtual Machine ... 2297
Configure a Virtual Machine to Use PVRDMA Native Endpoints ... 2298
Network Requirements for RDMA over Converged Ethernet ... 2299
Configure Remote Direct Memory Access Network Adapters ... 2299
View RDMA Capable Network Adapter ... 2299
Configure Remote Direct Memory Access Network Adapters ... 2300
What are Jumbo Frames ... 2302
Enable Jumbo Frames on a vSphere Distributed Switch ... 2303
Enable Jumbo Frames on a vSphere Standard Switch ... 2303
Enable Jumbo Frames for a VMkernel Adapter ... 2303
Enable Jumbo Frame Support on a Virtual Machine ... 2304
TCP Segmentation Offload ... 2304
Enable or Disable Software TSO in the VMkernel ... 2304
Determine Whether TSO Is Supported on the Physical Network Adapters on an ESXi Host ... 2305
Enable or Disable TSO on an ESXi Host ... 2305
Determine Whether TSO Is Enabled on an ESXi Host ... 2306
Manage TSO on a Linux Virtual Machine ... 2306
Manage TSO on a Windows Virtual Machine ... 2306
Large Receive Offload ... 2306
Manage Hardware LRO for All VMXNET3 Adapters on an ESXi Host ... 2307
Manage Software LRO for All VMXNET3 Adapters on an ESXi Host ... 2307
Determine Whether LRO Is Enabled for VMXNET3 Adapters on an ESXi Host ... 2307
Change the Size of the LRO Buffer for VMXNET 3 Adapters ... 2308
Enable or Disable LRO for All VMkernel Adapters on an ESXi Host ... 2308
Change the Size of the LRO Buffer for VMkernel Adapters ... 2308
Manage LRO on a VMXNET3 Adapter on a Linux Virtual Machine ... 2309
Enable or Disable LRO on a VMXNET3 Adapter on a Windows Virtual Machine ... 2309
Enable LRO Globally on a Windows Virtual Machine ... 2309
NetQueue and Networking Performance ... 2310
Activate NetQueue on a Host ... 2310
Deactivate NetQueue on a Host ... 2310
vSphere Network I/O Control ... 2311
About vSphere Network I/O Control Version 3 ... 2311
Enable Network I/O Control on a vSphere Distributed Switch ... 2311
Bandwidth Allocation for System Traffic ... 2311
Bandwidth Allocation Parameters for System Traffic ... 2312
Example Bandwidth Reservation for System Traffic ... 2313
Configure Bandwidth Allocation for System Traffic ... 2313

Bandwidth Allocation for Virtual Machine Traffic 2314
About Allocating Bandwidth for Virtual Machines 2314
Bandwidth Allocation Parameters for Virtual Machine Traffic 2316
Admission Control for Virtual Machine Bandwidth 2317
Create a Network Resource Pool 2318
Add a Distributed Port Group to a Network Resource Pool 2318
Configure Bandwidth Allocation for a Virtual Machine 2319
Configure Bandwidth Allocation on Multiple Virtual Machines 2320
Change the Quota of a Network Resource Pool 2320
Remove a Distributed Port Group from a Network Resource Pool 2321
Delete a Network Resource Pool 2321
Move a Physical Adapter Out the Scope of Network I/O Control 2321
MAC Address Management 2322
MAC Address Assignment from vCenter Server 2322
VMware OUI Allocation 2323
Prefix-Based MAC Address Allocation 2323
Range-Based MAC Address Allocation 2324
Assigning a MAC Address 2324
MAC Address Generation on ESXi Hosts 2326
Setting a Static MAC Address to a Virtual Machine 2326
VMware OUI in Static MAC Addresses 2327
Assign a Static MAC Address 2327
Assign a Static MAC Address in the Virtual Machine Configuration File 2328
Configuring vSphere for IPv6 2328
vSphere IPv6 Connectivity 2328
Deploying vSphere on IPv6 2330
Enable IPv6 on a vSphere Installation 2330
Enable IPv6 on an Upgraded vSphere Environment 2331
Activate or Deactivate IPv6 Support on a Host 2332
Set Up IPv6 on an ESXi Host 2332
Set Up IPv6 on vCenter Server 2333
Monitoring Network Connection and Traffic 2334
Capture Network Packets by Using the PacketCapture Utility 2334
Capturing and Tracing Network Packets by Using the pktcap-uw Utility 2335
pktcap-uw Command Syntax for Capturing Packets 2336
pktcap-uw Command Syntax for Tracing Packets 2337
pktcap-uw Options for Output Control 2338
pktcap-uw Options for Filtering Packets 2339
Capturing Packets by Using the pktcap-uw Utility 2340
Trace Packets by Using the pktcap-uw Utility 2349

Configure the NetFlow Settings of a vSphere Distributed Switch.....2350
Working With Port Mirroring.....2351
Port Mirroring Interoperability.....2351
Create a Port Mirroring Session.....2352
View Port Mirroring Session Details.....2356
Edit Port Mirroring Session Details, Sources, and Destinations.....2356
vSphere Distributed Switch Health Check.....2357
Manage vSphere Distributed Switch Health Check.....2358
View vSphere Distributed Switch Health Status.....2358
Switch Discovery Protocol.....2358
Enable Cisco Discovery Protocol on a vSphere Distributed Switch.....2359
Enable Link Layer Discovery Protocol on a vSphere Distributed Switch.....2359
View Switch Information.....2360
View the Topology Diagram of an NSX Virtual Distributed Switch.....2360
Configuring Protocol Profiles for Virtual Machine Networking.....2360
Add a Network Protocol Profile.....2361
Select the Network Protocol Profile Name and Network.....2363
Specify Network Protocol Profile IPv4 Configuration.....2363
Specify Network Protocol Profile IPv6 Configuration.....2363
Specify Network Protocol Profile DNS and Other Configuration.....2364
Complete the Network Protocol Profile Creation.....2364
Associate a Port Group with a Network Protocol Profile.....2364
Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp.....2365
Multicast Filtering.....2366
Multicast Filtering Modes.....2366
Enable Multicast Snooping on a vSphere Distributed Switch.....2367
Edit the Query Time Interval for Multicast Snooping.....2368
Edit the Number of Source IP Addresses for IGMP and MLD.....2368
What is Stateless Network Deployment.....2369
Networking Best Practices.....2370
Troubleshooting Networking.....2370
Guidelines for Troubleshooting.....2371
Identifying Symptoms.....2371
Defining the Problem Space.....2371
Testing Possible Solutions.....2372
Troubleshooting with vCenter Server Logs.....2372
Troubleshooting MAC Address Allocation.....2373
Duplicate MAC Addresses of Virtual Machines on the Same Network.....2373
Attempt to Power On a Virtual Machine Fails Due to a MAC Address Conflict.....2375
Unable to Remove a Host from a vSphere Distributed Switch.....2376

Hosts on a vSphere Distributed Switch Lose Connectivity to vCenter Server 2376
Alarm for Loss of Network Redundancy on a Host 2377
Virtual Machines Lose Connectivity After Changing the Uplink Failover Order of a Distributed Port Group 2378
Unable to Add a Physical Adapter to a vSphere Distributed Switch 2379
Troubleshooting SR-IOV Enabled Workloads 2379
SR-IOV Enabled Workload Cannot Communicate After You Change Its MAC Address 2379
A Virtual Machine that Runs a VPN Client Causes Denial of Service for Virtual Machines on the Host or Across a vSphere HA Cluster 2380
Low Throughput for UDP Workloads on Windows Virtual Machines 2381
VMs on the Same Distributed Port Group are Unable to Communicate 2383
Attempt to Power On a Migrated vApp Fails Because the Associated Protocol Profile Is Missing 2384
Networking Configuration Operation Is Rolled Back and a Host Is Disconnected from vCenter Server 2384
vSphere Storage 2386
Updated Information 2386
Introduction to Storage 2387
Traditional Storage Virtualization Models 2387
Software-Defined Storage Models 2389
vSphere Storage APIs 2389
Getting Started with a Traditional Storage Model 2390
Types of Physical Storage 2390
Local Storage 2390
Networked Storage 2391
Target and Device Representations 2394
How Virtual Machines Access Storage 2395
Storage Device Characteristics 2396
Comparing Types of Storage 2399
Supported Storage Adapters 2400
View Storage Adapter Information 2400
Datastore Characteristics 2401
Display Datastore Information 2402
Using Persistent Memory Devices with ESXi 2403
Monitor PMem Datastore Statistics 2405
Overview of Using ESXi with a SAN 2406
ESXi and SAN Use Cases 2406
Specifics of Using SAN Storage with ESXi 2407
ESXi Hosts and Multiple Storage Arrays 2407
Making LUN Decisions 2407
Use the Predictive Scheme to Make LUN Decisions 2408
Use the Adaptive Scheme to Make LUN Decisions 2408
Selecting Virtual Machine Locations 2408

Third-Party Management Applications....2409
SAN Storage Backup Considerations....2409
Using Third-Party Backup Packages....2410
Using ESXi with Fibre Channel SAN....2410
Fibre Channel SAN Concepts....2410
Ports in Fibre Channel SAN....2411
Fibre Channel Storage Array Types....2411
Using Zoning with Fibre Channel SANs....2411
How Virtual Machines Access Data on a Fibre Channel SAN....2412
Configuring Fibre Channel Storage....2412
ESXi Fibre Channel SAN Requirements....2412
ESXi Fibre Channel SAN Restrictions....2412
Setting LUN Allocations....2413
Setting Fibre Channel HBAs....2413
Installation and Setup Steps....2413
N-Port ID Virtualization....2414
How NPIV-Based LUN Access Works....2414
Requirements for Using NPIV....2414
NPIV Capabilities and Limitations....2414
Configure or Modify WWN Assignments....2415
Configuring Fibre Channel over Ethernet....2415
Fibre Channel over Ethernet Adapters....2416
Configuration Guidelines for Software FCoE....2416
Set Up Networking for Software FCoE....2417
Add Software FCoE Adapters....2418
Booting ESXi from Fibre Channel SAN....2418
Boot from SAN Benefits....2418
Requirements and Considerations when Booting from Fibre Channel SAN....2419
Getting Ready for Boot from SAN....2419
Configure SAN Components and Storage System....2419
Configure Storage Adapter to Boot from SAN....2420
Set Up Your System to Boot from Installation Media....2420
Configure Emulex HBA to Boot from SAN....2420
Enable the BootBIOS Prompt....2421
Enable the BIOS....2421
Configure QLogic HBA to Boot from SAN....2421
Booting ESXi with Software FCoE....2422
Requirements and Considerations for Software FCoE Boot....2422
Set Up Software FCoE Boot....2423
Configure Software FCoE Boot Parameters....2423

Install and Boot ESXifrom Software FCoE LUN..... 2423
Troubleshooting Boot from Software FCoE for an ESXi Host..... 2424
Best Practices for Fibre Channel Storage..... 2424
Preventing Fibre Channel SAN Problems..... 2424
Disable Automatic ESXi Host Registration..... 2425
Optimizing Fibre Channel SAN Storage Performance..... 2425
Storage Array Performance..... 2425
Server Performance with Fibre Channel..... 2426
Using ESXi with iSCSI SAN..... 2426
About iSCSI SAN..... 2426
iSCSI Multipathing..... 2427
Nodes and Ports in the iSCSI SAN..... 2427
iSCSI Naming Conventions..... 2428
iSCSI Initiators..... 2428
Using iSER Protocol with ESXi..... 2429
Establishing iSCSI Connections..... 2430
iSCSI Storage System Types..... 2430
Discovery, Authentication, and Access Control..... 2431
How Virtual Machines Access Data on an iSCSI SAN..... 2431
Error Correction..... 2432
Configuring iSCSI and iSER Adapters and Storage..... 2432
ESXi iSCSI SAN Recommendations and Restrictions..... 2433
Configuring iSCSI Parameters for Adapters..... 2433
Set Up Independent Hardware iSCSI Adapters..... 2434
View Independent Hardware iSCSI Adapters..... 2435
Edit Network Settings for Hardware iSCSI..... 2436
Configure Dependent Hardware iSCSI Adapters..... 2436
Dependent Hardware iSCSI Considerations..... 2437
View Dependent Hardware iSCSI Adapters..... 2438
Determine Association Between iSCSI and Network Adapters..... 2438
Configure the Software iSCSI Adapter..... 2438
Activate or Disable the Software iSCSI Adapter..... 2439
Configure iSER with ESXi..... 2440
Install and View an RDMA Capable Network Adapter..... 2441
Enable the VMware iSER Adapter..... 2441
Modify General Properties for iSCSI or iSER Adapters..... 2443
Setting Up Network for iSCSI and iSER..... 2443
Multiple Network Adapters in iSCSI or iSER Configuration..... 2444
Best Practices for Configuring Networking with Software iSCSI..... 2446
Configure Port Binding for iSCSI or iSER..... 2450

Managing iSCSI Network ... 2452
iSCSI Network Troubleshooting ... 2453
Using Jumbo Frames with iSCSI and iSER ... 2453
Enable Jumbo Frames for Networking ... 2454
Enable Jumbo Frames for Independent Hardware iSCSI ... 2454
Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host ... 2454
Remove Dynamic or Static iSCSI Targets ... 2455
Configuring CHAP Parameters for iSCSI or iSER Storage Adapters ... 2456
Selecting CHAP Authentication Method ... 2456
Set Up CHAP for iSCSI or iSER Storage Adapter ... 2457
Set Up CHAP for Target ... 2458
Configuring Advanced Parameters for iSCSI ... 2459
Configure Advanced Parameters for iSCSI on ESXi Host ... 2460
iSCSI Session Management ... 2460
Review iSCSI Sessions ... 2461
Add iSCSI Sessions ... 2461
Remove iSCSI Sessions ... 2461
Booting from iSCSI SAN with ESXi ... 2462
General Recommendations for Boot from iSCSI SAN ... 2462
Prepare the iSCSI SAN ... 2463
Configure Independent Hardware iSCSI Adapter for SAN Boot ... 2463
Configure iSCSI Boot Settings ... 2464
Best Practices for iSCSI Storage ... 2464
Preventing iSCSI SAN Problems ... 2464
Optimizing iSCSI SAN Storage Performance ... 2465
Storage System Performance ... 2465
Server Performance with iSCSI ... 2465
Network Performance ... 2466
Checking Ethernet Switch Statistics ... 2468
Managing Storage Devices ... 2468
Storage Device Characteristics ... 2468
Display Storage Devices for an ESXi Host ... 2469
Display Storage Devices for an Adapter ... 2470
Device Sector Formats ... 2471
Storage Device Names and Identifiers ... 2472
NVMe Devices with NGUID Device Identifiers ... 2473
Upgrade Stateless ESXi Hosts with NGUID-only NVMe Devices to Version 7.0.x ... 2474
Rename Storage Devices ... 2476
Storage Rescan Operations ... 2476
Perform Storage Rescan ... 2476

Perform Adapter Rescan ... 2477
Change the Number of Scanned Storage Devices ... 2477
Identifying Device Connectivity Problems ... 2477
Detecting PDL Conditions ... 2478
Performing Planned Storage Device Removal ... 2479
Recovering from PDL Conditions ... 2480
Handling Transient APD Conditions ... 2480
Verify the Connection Status of a Storage Device on ESXi Host ... 2482
Enable or Disable Locator LED on ESXi Storage Devices ... 2482
Erase Storage Devices ... 2482
Change Perennial Reservation Settings ... 2483
Working with Flash Devices ... 2484
Marking Storage Devices ... 2484
Mark Storage Devices as Flash ... 2485
Mark Storage Devices as Local ... 2485
Monitor Flash Devices ... 2485
Best Practices for Flash Devices ... 2486
Estimate Lifetime of Flash Devices ... 2486
About Virtual Flash Resource ... 2486
Considerations for Virtual Flash Resource ... 2487
Set Up Virtual Flash Resource ... 2487
Remove Virtual Flash Resource ... 2488
Set Alarm for Virtual Flash Use ... 2488
Configure Host Cache with VMFS Datastore ... 2488
Keeping Flash Disks VMFS-Free ... 2489
About VMware NVMe Storage ... 2489
VMware NVMe Concepts ... 2489
Basic VMware NVMe Architecture and Components ... 2491
Requirements and Limitations of VMware NVMe Storage ... 2494
Configuring Lossless Ethernet for NVMe over RDMA ... 2496
Configure Adapters for NVMe over RDMA (RoCE v2) Storage ... 2497
View RDMA Network Adapters ... 2497
Configure VMkernel Binding for the RDMA Adapter ... 2497
Configure Adapters for NVMe over TCP Storage ... 2503
Configure VMkernel Binding for the NVMe over TCP Adapter ... 2503
Enable NVMe over RDMA or NVMe over TCP Software Adapters ... 2508
Add Controller for NVMe over Fabrics ... 2509
Remove NVMe over RDMA and TCP Software Adapters ... 2510
Working with Datastores ... 2510
Types of Datastores ... 2510

Understanding VMFS Datastores 2511
Versions of VMFS Datastores 2511
VMFS Datastores as Repositories 2513
Sharing a VMFS Datastore Across Hosts 2513
VMFS Metadata Updates 2514
VMFS Locking Mechanisms 2514
Snapshot Formats on VMFS 2517
Upgrading VMFS Datastores 2518
Understanding Network File System Datastores 2518
NFS Protocols and ESXi 2519
NFS Storage Guidelines and Requirements 2520
Firewall Configurations for NFS Storage 2522
Using Layer 3 Routed Connections to Access NFS Storage 2523
Using Kerberos for NFS 4.1 2524
Set Up NFS Storage Environment 2524
Configure ESXi Hosts for Kerberos Authentication 2525
Collecting Statistical Information for NFS Storage 2526
Creating Datastores 2527
Create a VMFS Datastore 2527
Create an NFS Datastore 2528
Create a Virtual Volumes Datastore 2529
Managing Duplicate VMFS Datastores 2529
Mount a VMFS Datastore Copy 2530
Increase VMFS Datastore Capacity 2531
Enable or Disable Support for Clustered Virtual Disks on the VMFS6 Datastore 2532
Administrative Operations for Datastores 2532
Change Datastore Name 2533
Unmount Datastores 2533
Mount Datastores 2533
Remove VMFS Datastores 2534
Use Datastore Browser 2534
Turn Off Storage Filters 2537
Set Up Dynamic Disk Mirroring 2538
Collecting Diagnostic Information for ESXi Hosts on a VMFS Datastore 2539
Set Up a File as Core Dump Location 2539
Deactivate and Delete a Core Dump File 2540
Checking Metadata Consistency with VOMA 2541
Use VOMA to Check Metadata Consistency 2543
Configuring VMFS Pointer Block Cache 2543
Obtain Information for VMFS Pointer Block Cache 2544

Change the Size of the Pointer Block Cache 2545
Understanding Multipathing and Failover 2545
Failovers with Fibre Channel 2545
Host-Based Failover with iSCSI 2546
Array-Based Failover with iSCSI 2547
Path Failover and Virtual Machines 2549
Set Timeout on Windows Guest OS 2549
Pluggable Storage Architecture and Path Management 2549
About Pluggable Storage Architecture 2550
VMware Native Multipathing Plug-In 2551
Path Selection Plug-Ins and Policies 2553
VMware SATPs 2554
VMware High Performance Plug-In and Path Selection Schemes 2555
Viewing and Managing Paths 2560
View Storage Device Paths 2561
View Datastore Paths 2561
Change the Path Selection Policy 2563
Change Default Parameters for Latency Round Robin 2564
Disable Storage Paths 2565
Using Claim Rules 2565
Multipathing Considerations 2565
List Multipathing Claim Rules for the Host 2566
Add Multipathing Claim Rules 2567
Delete Multipathing Claim Rules 2570
Mask Paths 2571
Unmask Paths 2571
Define NMP SATP Rules 2572
Scheduling Queues for Virtual Machine I/Os 2573
Edit Per File I/O Scheduling in the vSphere Client 2573
Use esxcli Commands to Enable or Disable Per File I/O Scheduling 2574
Raw Device Mapping 2574
About Raw Device Mapping 2574
Benefits of Raw Device Mapping 2575
RDM Considerations and Limitations 2577
Raw Device Mapping Characteristics 2577
RDM Virtual and Physical Compatibility Modes 2577
Dynamic Name Resolution 2578
Raw Device Mapping with Virtual Machine Clusters 2578
Comparing Available SCSI Device Access Modes 2578
Create Virtual Machines with RDMs 2579

Manage Paths for a Mapped LUN....2580
Virtual Machines with RDMs Must Ignore SCSI INQUIRY Cache....2581
Storage Policy Based Management....2581
Virtual Machine Storage Policies....2582
Workflow for Virtual Machine Storage Policies....2582
Populating the VM Storage Policies Interface....2583
Use Storage Providers to Populate the VM Storage Policies Interface....2584
Assign Tags to Datastores....2585
About Rules and Rule Sets....2586
Creating and Managing VM Storage Policies....2587
Create a VM Storage Policy for Host-Based Data Services....2588
Create a VM Storage Policy for Virtual Volumes....2589
Create a VM Storage Policy for Tag-Based Placement....2590
Edit or Clone a VM Storage Policy....2591
About Storage Policy Components....2592
Create Storage Policy Components....2593
Edit or Clone Storage Policy Components....2593
Storage Policies and Virtual Machines....2594
Assign Storage Policies to Virtual Machines....2594
Change Storage Policy Assignment for Virtual Machine Files and Disks....2595
Check Compliance for a VM Storage Policy....2596
Find Compatible Storage Resource for Noncompliant Virtual Machine....2597
Reapply Virtual Machine Storage Policy....2597
Default Storage Policies....2598
Change the Default Storage Policy for a Datastore....2599
Using Storage Providers....2599
About Storage Providers....2599
Storage Providers and Data Representation....2600
Storage Provider Requirements and Considerations....2601
Register Storage Providers....2601
View Storage Provider Information....2602
Manage Storage Providers....2602
Working with VMware vSphere Virtual Volumes....2603
About Virtual Volumes....2603
Virtual Volumes Concepts....2603
Virtual Volume Objects....2604
Virtual Volumes Storage Providers....2605
Virtual Volumes Storage Containers....2606
Protocol Endpoints....2607
Binding and Unbinding Virtual Volumes to Protocol Endpoints....2608

Virtual Volumes Datastores....2609
Virtual Volumes and VM Storage Policies....2610
Virtual Volumes and Storage Protocols....2610
Virtual Volumes Architecture....2612
Virtual Volumes and VMware Certificate Authority....2613
Virtual Volume Snapshots....2613
Before You Enable Virtual Volumes....2614
Synchronize vSphere Storage Environment with a Network Time Server....2615
Configure Virtual Volumes....2615
Register Storage Providers for Virtual Volumes....2615
Create a Virtual Volumes Datastore....2616
Review and Manage Protocol Endpoints....2617
Change the Path Selection Policy for a Protocol Endpoint....2617
Provision Virtual Machines on Virtual Volumes Datastores....2617
Virtual Volumes and Replication....2618
Requirements for Replication with Virtual Volumes....2619
Virtual Volumes and Replication Groups....2620
Virtual Volumes and Fault Domains....2620
Virtual Volumes Replication Workflow....2622
Replication Guidelines and Considerations....2622
Best Practices for Working with Virtual Volumes....2623
Guidelines and Limitations when Using Virtual Volumes....2623
Best Practices for Storage Container Provisioning....2624
Best Practices for Virtual Volumes Performance....2625
Troubleshooting Virtual Volumes....2625
Virtual Volumes and esxcli Commands....2626
Collecting Statistical Information for Virtual Volumes....2626
Virtual Volumes Datastore Is Inaccessible....2627
Failures When Migrating VMs or Deploying VM OVFs to Virtual Volumes Datastores....2627
Filtering Virtual Machine I/O....2627
About I/O Filters....2628
Types of I/O Filters....2628
I/O Filtering Components....2628
Storage Providers for I/O Filters....2630
Using Flash Storage Devices with Cache I/O Filters....2630
System Requirements for I/O Filters....2631
Configure I/O Filters in the vSphere Environment....2631
Install I/O Filters in a Cluster....2631
View I/O Filters and Storage Providers....2632
Enable I/O Filter Data Services on Virtual Disks....2632

Assign the I/O Filter Policy to Virtual Machines....2632
Managing I/O Filters....2633
Uninstall I/O Filters from a Cluster....2633
Upgrade I/O Filters in a Cluster....2634
I/O Filter Guidelines and Best Practices....2634
Migrating Virtual Machines with I/O Filters....2635
Handling I/O Filter Installation Failures....2635
Install I/O Filters on a Single ESXi Host....2635
Storage Hardware Acceleration....2636
Hardware Acceleration Benefits....2636
Hardware Acceleration Requirements....2636
Hardware Acceleration Support Status....2636
Hardware Acceleration for Block Storage Devices....2637
Disable Hardware Acceleration for Block Storage Devices....2637
Managing Hardware Acceleration on Block Storage Devices....2637
Hardware Acceleration on NAS Devices....2641
Enable NAS Native Snapshots on Virtual Machines....2642
Hardware Acceleration Considerations....2643
Storage Provisioning and Space Reclamation....2643
Virtual Disk Thin Provisioning....2643
About Virtual Disk Provisioning Policies....2644
Create Thin Provisioned Virtual Disks....2645
View Virtual Machine Storage Resources....2645
Determine the Disk Format of a Virtual Machine....2646
Inflate Thin Virtual Disks....2646
Handling Datastore Over-Subscription....2646
ESXi and Array Thin Provisioning....2647
Monitoring Space Use....2647
Identify Thin-Provisioned Storage Devices....2648
Storage Space Reclamation....2648
Space Reclamation Requests from VMFS Datastores....2649
Space Reclamation Requests from Guest Operating Systems....2654
Getting Started with Cloud Native Storage....2654
Cloud Native Storage Concepts and Terminology....2655
Cloud Native Storage Components....2657
Using vSAN File Service to Provision File Volumes....2659
Cloud Native Storage Users....2661
Cloud Native Storage for vSphere Administrators....2662
Requirements of Cloud Native Storage....2662
Cloud Native Storage Roles and Privileges....2664

Create a Storage Policy for Kubernetes ... 2665
Configure Kubernetes Cluster Virtual Machines ... 2667
Monitor Container Volumes Across Kubernetes Clusters ... 2667
Use Encryption with Cloud Native Storage ... 2668
Migrating Container Volumes in vSphere ... 2669
Using vmkfstools ... 2672
vmkfstools Command Syntax ... 2672
The vmkfstools Command Options ... 2673
-v Suboption ... 2673
File System Options ... 2673
Virtual Disk Options ... 2675
Storage Device Options ... 2680
vSphere Security ... 2682
Updated Information ... 2683
Security in the vSphere Environment ... 2688
Securing the ESXi Hypervisor ... 2688
Securing vCenter Server Systems and Associated Services ... 2689
Securing Virtual Machines ... 2690
Securing the Virtual Networking Layer ... 2691
Passwords in Your vSphere Environment ... 2692
Security Best Practices and Resources ... 2693
vSphere Permissions and User Management Tasks ... 2694
Understanding Authorization in vSphere ... 2695
Hierarchical Inheritance of Permissions ... 2698
Multiple Permission Settings ... 2700
Managing Permissions for vCenter Components ... 2703
Add a Permission to an Inventory Object ... 2703
Change or Remove Permissions ... 2704
Change User Validation Settings ... 2704
Global Permissions ... 2704
Add a Global Permission ... 2705
Permissions on Tag Objects ... 2706
Using Roles to Assign Privileges ... 2707
Create a vCenter Server Custom Role ... 2708
vCenter Server System Roles ... 2709
Best Practices for Roles and Permissions ... 2709
Required vCenter Server Privileges for Common Tasks ... 2710
Securing ESXi Hosts ... 2713
General ESXi Security Recommendations ... 2713
Advanced System Settings ... 2714

Configure ESXi Hosts with Host Profiles 2717
Use Scripts to Manage Host Configuration Settings 2717
ESXi Passwords and Account Lockout 2718
Cryptographic Key Generation 2720
SSH Security 2721
PCI and PCIe Devices and ESXi 2722
Disable the Managed Object Browser 2723
ESXi Networking Security Recommendations 2723
Modifying ESXi Web Proxy Settings 2723
vSphere Auto Deploy Security Considerations 2724
Control Access for CIM-Based Hardware Monitoring Tools 2724
Certificate Management for ESXi Hosts 2725
Host Upgrades and Certificates 2727
Certificate Mode Switch Workflows 2727
ESXi Certificate Default Settings 2729
View Certificate Expiration Information for Multiple ESXi Hosts 2731
View Certificate Details for a Single ESXi Host 2731
Renew or Refresh ESXi Certificates 2732
Change the Certificate Mode 2732
Replacing ESXi SSL Certificates and Keys 2733
Use Custom Certificates with Auto Deploy 2736
Restore ESXi Certificate and Key Files 2737
Customizing Hosts with the Security Profile 2738
ESXi Firewall Configuration 2738
Customizing ESXi Services from the Security Profile 2741
Enable or Disable a Service 2742
Lockdown Mode 2743
Using VIBs to Perform Secure Updates 2747
Assigning Privileges for ESXi Hosts 2749
Using Active Directory to Manage ESXi Users 2751
Configure a Host to Use Active Directory 2751
Add a Host to a Directory Service Domain 2752
View Directory Service Settings 2752
Using vSphere Authentication Proxy 2753
Enable vSphere Authentication Proxy 2753
Add a Domain to vSphere Authentication Proxy with the vSphere Client 2754
Add a Domain to vSphere Authentication Proxy with the camconfig Command 2754
Use vSphere Authentication Proxy to Add a Host to a Domain 2755
Enable Client Authentication for vSphere Authentication Proxy 2755
Import the vSphere Authentication Proxy Certificate to ESXi Host 2756

Generate a New Certificate for vSphere Authentication Proxy....2756
Set Up vSphere Authentication Proxy to Use Custom Certificates....2757
Configuring Smart Card Authentication for ESXi....2758
Enable Smart Card Authentication....2758
Disable Smart Card Authentication....2759
Authenticating With User Name and Password in Case of Connectivity Problems....2759
Using Smart Card Authentication in Lockdown Mode....2759
Using the ESXi Shell....2760
Enable Access to the ESXi Shell....2760
Use the Direct Console User Interface to Enable Access to the ESXi Shell....2761
Log in to the ESXi Shell for Troubleshooting....2763
UEFI Secure Boot for ESXi Hosts....2763
Securing ESXi Hosts with Trusted Platform Module....2765
View ESXi Host Attestation Status....2766
Troubleshoot ESXi Host Attestation Problems....2766
ESXi Log Files....2766
Configure Syslog on ESXi Hosts....2767
ESXi Log File Locations....2767
Securing Fault Tolerance Logging Traffic....2768
Managing ESXi Audit Records....2769
Securing the ESXi Configuration....2769
Securing the ESXi Configuration Overview....2769
TPM Sealing Policies Overview....2771
Managing a Secure ESXi Configuration....2771
Securing vCenter Server Systems....2776
vCenter Server Security Best Practices....2776
Best Practices for vCenter Server Access Control....2777
Limiting vCenter Server Network Connectivity....2778
vCenter Server Security Best Practices....2780
vCenter Password Requirements and Lockout Behavior....2780
Verify Thumbprints for Legacy ESXi Hosts....2781
Required Ports for vCenter Server....2781
Securing Virtual Machines....2782
Activate or Deactivate UEFI Secure Boot for a Virtual Machine....2782
Virtual Machine Security Best Practices....2783
General Virtual Machine Protection....2783
Use Templates to Deploy Virtual Machines....2784
Minimize Use of the Virtual Machine Console....2784
Prevent Virtual Machines from Taking Over Resources....2784
Disable Unnecessary Functions Inside Virtual Machines....2785

Securing Virtual Machines with Intel Software Guard Extensions....2790
vSGX Overview....2790
Enable vSGX on a Virtual Machine....2791
Enable vSGX on an Existing Virtual Machine....2791
Remove vSGX from a Virtual Machine....2792
Securing Virtual Machines with AMD Secure Encrypted Virtualization-Encrypted State....2792
vSphere and AMD Secure Encrypted Virtualization-Encrypted State....2792
Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine with the vSphere Client....2793
Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine....2794
Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine with the vSphere Client....2795
Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine....2795
Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine with the vSphere Client....2796
Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine....2796
Virtual Machine Encryption....2797
Comparison of vSphere Key Providers....2797
How vSphere Virtual Machine Encryption Protects Your Environment....2799
vSphere Virtual Machine Encryption Components....2802
Encryption Process Flow....2804
Virtual Disk Encryption....2806
Virtual Machine Encryption Errors....2808
Prerequisites and Required Privileges for Encryption Tasks....2808
Encrypted vSphere vMotion....2809
Encryption Best Practices, Caveats, and Interoperability....2811
Virtual Machine Encryption Best Practices....2811
Virtual Machine Encryption Caveats....2814
Virtual Machine Encryption Interoperability....2815
Key Persistence Overview....2816
Configuring and Managing a Standard Key Provider....2817
Standard Key Provider Overview....2818
Set Up the Standard Key Provider....2818
Add a Standard Key Provider Using the vSphere Client....2818
Establish a Standard Key Provider Trusted Connection by Exchanging Certificates....2819
Set the Default Key Provider....2822
Finish the Trust Setup for a Standard Key Provider....2822
Set Up Separate Key Providers for Different Users....2823
Delete a Standard Key Provider....2823
Configuring and Managing vSphere Native Key Provider....2824
vSphere Native Key Provider Overview....2824

vSphere Native Key Provider Process Flows....2826
Configure a vSphere Native Key Provider....2827
Back up a vSphere Native Key Provider....2828
Recovering a vSphere Native Key Provider....2828
Restore a vSphere Native Key Provider Using the vSphere Client....2829
Update a vSphere Native Key Provider....2829
Delete a vSphere Native Key Provider....2830
vSphere Trust Authority....2831
vSphere Trust Authority Concepts and Features....2831
How vSphere Trust Authority Protects Your Environment....2831
Trusted Infrastructure Overview....2834
vSphere Trust Authority Process Flows....2836
vSphere Trust Authority Topology....2839
Prerequisites and Required Privileges for vSphere Trust Authority....2839
vSphere Trust Authority Best Practices, Caveats, and Interoperability....2841
vSphere Trust Authority Life Cycle....2842
Configuring vSphere Trust Authority....2844
Set up Your Workstation....2846
Enable the Trust Authority Administrator....2846
Enable the Trust Authority State....2847
Collect Information About ESXi Hosts and vCenter Server to Be Trusted....2848
Import the Trusted Host Information to the Trust Authority Cluster....2855
Create the Key Provider on the Trust Authority Cluster....2857
Export the Trust Authority Cluster Information....2864
Import the Trust Authority Cluster Information to the Trusted Hosts....2865
Configure the Trusted Key Provider for Trusted Hosts Using the vSphere Client....2869
Configure the Trusted Key Provider for Trusted Hosts Using the Command Line....2869
Managing vSphere Trust Authority in Your vSphere Environment....2870
Start, Stop, and Restart vSphere Trust Authority Services....2871
View the Trust Authority Hosts....2871
View the vSphere Trust Authority Cluster State....2871
Restart the Trusted Host Service....2871
Adding and Removing vSphere Trust Authority Hosts....2872
Add a Host to a Trusted Cluster with the vSphere Client....2872
Add a Host to a Trusted Cluster with the CLI....2872
Decommission Trusted Hosts from a Trusted Cluster....2873
Backing Up the vSphere Trust Authority Configuration....2874
Change the Primary Key of a Key Provider....2874
Trusted Host Attestation Reporting Overview....2875
Checking and Remediating Trusted Cluster Health....2877

Use Encryption in Your vSphere Environment....2879
Create an Encryption Storage Policy....2879
Enable Host Encryption Mode Explicitly....2880
Disable Host Encryption Mode Using the API....2880
Create an Encrypted Virtual Machine....2881
Clone an Encrypted Virtual Machine....2882
Encrypt an Existing Virtual Machine or Virtual Disk....2883
Decrypt an Encrypted Virtual Machine or Virtual Disk....2884
Change the Encryption Policy for Virtual Disks....2885
Resolve Missing Key Issues....2885
Unlock Locked Virtual Machines....2887
Resolve ESXi Host Encryption Mode Issues....2887
Re-Enable ESXi Host Encryption Mode....2887
Set Key Management Server Certificate Expiration Threshold....2888
vSphere Virtual Machine Encryption and Core Dumps....2888
Collect a vm-support Package for an ESXi Host That Uses Encryption....2889
Decrypt or Re-Encrypt an Encrypted Core Dump....2890
Enable and Disable Key Persistence on an ESXi Host....2891
Rekey an Encrypted Virtual Machine Using the vSphere Client....2891
Securing Virtual Machines with Virtual Trusted Platform Module....2892
Virtual Trusted Platform Module Overview....2892
Create a Virtual Machine with a Virtual Trusted Platform Module....2893
Enable Virtual Trusted Platform Module for an Existing Virtual Machine....2894
Remove Virtual Trusted Platform Module from a Virtual Machine....2895
Identify Virtual Trusted Platform Module Enabled Virtual Machines....2895
View Virtual Trusted Platform Module Device Certificates....2896
Export and Replace Virtual Trusted Platform Module Device Certificates....2896
Securing Windows Guest Operating Systems with Virtualization-based Security....2897
Virtualization-based Security Best Practices....2897
Enable Virtualization-based Security on a Virtual Machine....2898
Enable Virtualization-based Security on an Existing Virtual Machine....2899
Enable Virtualization-based Security on the Guest Operating System....2900
Deactivate Virtualization-based Security....2900
Identify VBS-Enabled Virtual Machines....2901
Securing vSphere Networking....2901
Introduction to vSphere Network Security....2901
Securing the Network with Firewalls....2902
Firewalls for Configurations with vCenter Server....2903
Connecting to vCenter Server Through a Firewall....2903
Connecting ESXi Hosts Through Firewalls....2903

Firewalls for Configurations Without vCenter Server ... 2903
Connecting to the Virtual Machine Console Through a Firewall ... 2904
Secure the Physical Switch ... 2905
Securing Standard Switch Ports with Security Policies ... 2905
Securing vSphere Standard Switches ... 2905
MAC Address Changes ... 2906
Forged Transmits ... 2907
Promiscuous Mode Operation ... 2907
Standard Switch Protection and VLANs ... 2907
Secure vSphere Distributed Switches and Distributed Port Groups ... 2908
Securing Virtual Machines with VLANs ... 2909
Security Considerations for VLANs ... 2910
Secure VLANs ... 2911
Creating Multiple Networks Within a Single ESXi Host ... 2911
Internet Protocol Security ... 2913
List Available Security Associations ... 2913
Add an IPsec Security Association ... 2913
Remove an IPsec Security Association ... 2914
List Available IPsec Security Policies ... 2915
Create an IPSec Security Policy ... 2915
Remove an IPsec Security Policy ... 2916
Ensure Proper SNMP Configuration ... 2916
vSphere Networking Security Best Practices ... 2916
General Networking Security Recommendations ... 2916
Labeling Networking Components ... 2917
Document and Check the vSphere VLAN Environment ... 2918
Adopting Network Isolation Practices ... 2918
Use Virtual Switches with the vSphere Network Appliance API Only If Required ... 2919
Best Practices Involving Multiple vSphere Components ... 2920
Synchronizing Clocks on the vSphere Network ... 2920
Synchronize ESXi Clocks with a Network Time Server ... 2921
Configuring Time Synchronization Settings in vCenter Server ... 2921
Storage Security Best Practices ... 2923
Securing iSCSI Storage ... 2923
Masking and Zoning SAN Resources ... 2924
Using Kerberos for NFS 4.1 ... 2924
Verify That Sending Host Performance Data to Guests Is Disabled ... 2925
Setting Timeouts for the ESXi Shell and vSphere Client ... 2926
Managing TLS Protocol Configuration with the TLS Configurator Utility ... 2926
Ports That Support Disabling TLS Versions ... 2926

Enabling or Disabling TLS Versions in vSphere ... 2927
Perform an Optional Manual Backup ... 2927
Enable or Disable TLS Versions on vCenter Server Systems ... 2928
Enable or Disable TLS Versions on ESXi Hosts ... 2928
Scan vCenter Server for Enabled TLS Protocols ... 2929
Revert TLS Configuration Changes ... 2930
Defined Privileges ... 2930
Alarms Privileges ... 2931
Auto Deploy and Image Profile Privileges ... 2931
Certificates Privileges ... 2932
Certificate Authority Privileges ... 2932
Certificate Management Privileges ... 2932
Cns Privileges ... 2933
Content Library Privileges ... 2933
Cryptographic Operations Privileges ... 2935
dvPort Group Privileges ... 2936
Distributed Switch Privileges ... 2937
Datacenter Privileges ... 2937
Datastore Privileges ... 2938
Datastore Cluster Privileges ... 2939
ESX Agent Manager Privileges ... 2939
Extension Privileges ... 2939
External Stats Provider Privileges ... 2940
Folder Privileges ... 2940
Global Privileges ... 2940
Health Update Provider Privileges ... 2941
Host CIM Privileges ... 2941
Host Configuration Privileges ... 2942
Host Inventory ... 2943
Host Local Operations Privileges ... 2943
Host vSphere Replication Privileges ... 2944
Host Profile Privileges ... 2944
vSphere with Tanzu Privileges ... 2945
Network Privileges ... 2945
Performance Privileges ... 2946
Permissions Privileges ... 2946
Profile-driven Storage Privileges ... 2947
Resource Privileges ... 2947
Scheduled Task Privileges ... 2948
Sessions Privileges ... 2948

Storage Views Privileges 2948
Tasks Privileges 2949
Transfer Service Privileges 2949
VcTrusts/VcIdentity Privileges 2949
Trusted Infrastructure Administrator Privileges 2949
vApp Privileges 2950
VcIdentityProviders Privileges 2951
VMware vSphere Lifecycle Manager Configuration Privileges 2952
VMware vSphere Lifecycle Manager ESXi Health Perspectives Privileges 2952
VMware vSphere Lifecycle Manager General Privileges 2953
VMware vSphere Lifecycle Manager Hardware Compatibility Privileges 2953
VMware vSphere Lifecycle Manager Image Privileges 2953
VMware vSphere Lifecycle Manager Image Remediation Privileges 2954
VMware vSphere Lifecycle Manager Settings Privileges 2954
VMware vSphere Lifecycle Manager Manage Baseline Privileges 2955
VMware vSphere Lifecycle Manager Manage Patches and Upgrades Privileges 2955
VMware vSphere Lifecycle Manager Upload File Privileges 2956
Virtual Machine Configuration Privileges 2956
Virtual Machine Guest Operations Privileges 2958
Virtual Machine Interaction Privileges 2959
Virtual Machine Inventory Privileges 2961
Virtual Machine Provisioning Privileges 2961
Virtual Machine Service Configuration Privileges 2962
Virtual Machine Snapshot Management Privileges 2963
Virtual Machine vSphere Replication Privileges 2963
vServices Privileges 2964
vSphere Tagging Privileges 2964
vSphere Client Privileges 2965
Understanding vSphere Hardening and Compliance 2965
Security Versus Compliance in the vSphere Environment 2965
Understanding the vSphere Security Configuration Guide 2967
About the National Institute of Standards and Technology 2969
About DISA STIGs 2969
About VMware Security Development Lifecycle 2970
Audit Logging 2970
Single Sign-On Audit Events 2970
Understanding Security and Compliance Next Steps 2971
vCenter Server and FIPS 2972
FIPS Modules 2972
Enable and Disable FIPS on the vCenter Server Appliance 2973

Considerations When Using FIPS....2973
vSphere Resource Management....2975
Getting Started with Resource Management....2975
Resource Types....2975
Resource Providers....2975
Resource Consumers....2976
Goals of Resource Management....2976
Configuring Resource Allocation Settings....2976
Resource Allocation Shares....2977
Resource Allocation Reservation....2977
Resource Allocation Limit....2978
Resource Allocation Settings Suggestions....2978
Edit Settings....2979
Changing Resource Allocation Settings—Example....2979
Admission Control....2980
CPU Virtualization Basics....2980
Software-Based CPU Virtualization....2981
Hardware-Assisted CPU Virtualization....2981
Virtualization and Processor-Specific Behavior....2981
Performance Implications of CPU Virtualization....2981
Administering CPU Resources....2982
View Processor Information....2982
Specifying CPU Configuration....2982
Multicore Processors....2982
Hyperthreading with vSphere....2983
Hyperthreading and ESXi Hosts....2983
Enable Hyperthreading....2984
Using CPU Affinity....2984
Assign a Virtual Machine to a Specific Processor....2985
Potential Issues with CPU Affinity....2985
Host Power Management Policies....2985
Select a CPU Power Management Policy....2986
Configure Custom Policy Parameters for Host Power Management....2986
Memory Virtualization Basics....2987
Virtual Machine Memory....2987
Memory Overcommitment....2988
Memory Sharing....2988
Memory Virtualization....2989
Hardware-Assisted Memory Virtualization....2990
Support for Large Page Sizes....2990

Administering Memory Resources **2991**
Understanding Memory Overhead 2991
Overhead Memory on Virtual Machines 2991
How ESXi Hosts Allocate Memory 2992
Memory Tax for Idle Virtual Machines 2992
VMX Swap Files 2992
Memory Reclamation 2993
Memory Balloon Driver 2993
Using Swap Files 2994
Swap File Location 2994
Enable Host-Local Swap for a DRS Cluster 2994
Enable Host-Local Swap for a Standalone Host 2995
Swap Space and Memory Overcommitment 2995
Configure Virtual Machine Swapfile Properties for the Host 2995
Configure a Virtual Machine Swap File Location for a Cluster 2996
Delete Swap Files 2997
Sharing Memory Across Virtual Machines 2997
Memory Compression 2998
Activate or Deactivate the Memory Compression Cache 2998
Set the Maximum Size of the Memory Compression Cache 2998
Measuring and Differentiating Types of Memory Usage 2999
Memory Reliability 3000
Correcting an Error Isolation Notification 3000
About System Swap 3000
Configure System Swap 3001
Persistent Memory **3001**
Configure vSphere HA for PMem VMs 3002
vSphere HA Admission Control PMem Reservation 3003
vSphere Memory Monitoring and Remediation 3003
Configuring Virtual Graphics **3005**
View GPU Statistics 3005
Add an NVIDIA GRID vGPU to a Virtual Machine 3005
Configuring Host Graphics 3006
Configuring Graphics Devices 3006
Managing Storage I/O Resources **3006**
About Virtual Machine Storage Policies 3007
About I/O Filters 3007
Storage I/O Control Requirements 3007
Storage I/O Control Resource Shares and Limits 3008
View Storage I/O Control Shares and Limits 3008

Monitor Storage I/O Control Shares....3008
Set Storage I/O Control Resource Shares and Limits....3009
Enable Storage I/O Control....3009
Set Storage I/O Control Threshold Value....3010
Storage DRS Integration with Storage Profiles....3010
Managing Resource Pools....3011
Why Use Resource Pools?....3012
Create a Resource Pool....3013
Edit a Resource Pool....3015
Add a Virtual Machine to a Resource Pool....3015
Remove a Virtual Machine from a Resource Pool....3016
Remove a Resource Pool....3016
Resource Pool Admission Control....3016
Expandable Reservations Example 1....3017
Expandable Reservations Example 2....3017
Creating a DRS Cluster....3018
vSphere Cluster Services....3018
vCLS Datastore Placement....3020
Monitoring vSphere Cluster Services....3020
Maintaining Health of vSphere Cluster Services....3021
Putting a Cluster in Retreat Mode....3022
Retrieving Password for vCLS VMs....3022
vCLS VM Anti-Affinity Policies....3023
Admission Control and Initial Placement....3023
Single Virtual Machine Power On....3024
Group Power-on....3024
Virtual Machine Migration....3025
DRS Migration Threshold....3026
Migration Recommendations....3026
DRS Cluster Requirements....3026
Shared Storage Requirements....3026
Shared VMFS Volume Requirements....3027
Processor Compatibility Requirements....3027
vMotion Requirements for DRS Clusters....3028
Configuring DRS with Virtual Flash....3028
Create a Cluster....3028
Edit Cluster Settings....3029
Set a Custom Automation Level for a Virtual Machine....3031
Deactivate DRS....3031
Restore a Resource Pool Tree....3032

DRS Awareness of vSAN Stretched Cluster....3032
DRS Maintenance Mode Functionality with ROBO Enterprise License....3033
Limitations of DRS Maintenance Mode with ROBO Enterprise License....3033
Using DRS Maintenance Mode with ROBO Enterprise License....3033
Troubleshooting DRS Maintenance Mode with ROBO Enterprise License....3034
Using DRS Clusters to Manage Resources....3034
Adding Hosts to a Cluster....3034
Add a Managed Host to a Cluster....3035
Add an Unmanaged Host to a Cluster....3035
Adding Virtual Machines to a Cluster....3036
Move a Virtual Machine to a Cluster....3036
Removing Virtual Machines from a Cluster....3036
Move a Virtual Machine Out of a Cluster....3037
Removing a Host from a Cluster....3037
Place a Host in Maintenance Mode....3037
Remove a Host from a Cluster....3038
Using Standby Mode....3038
DRS Cluster Validity....3038
Valid DRS Clusters....3039
Overcommitted DRS Clusters....3041
Invalid DRS Clusters....3042
Managing Power Resources....3043
Configure IPMI or iLO Settings for vSphere DPM....3043
Test Wake-on-LAN for vSphere DPM....3044
Activating vSphere DPM for a DRS Cluster....3045
Monitoring vSphere DPM....3046
Using Affinity Rules with vSphere DRS....3047
VM-VM Affinity Rules with vSphere DRS....3047
VM-Host Affinity Rules with vSphere DRS....3047
Create a VM-Host Group....3048
Create a Virtual Machine Group....3049
Create a VM-VM Affinity Rule....3049
VM-VM Affinity Rule Conflicts....3049
Create a VM-Host Affinity Rule....3049
Using VM-Host Affinity Rules....3050
Using Affinity Rules without vSphere DRS....3051
Creating a Datastore Cluster....3052
Initial Placement and Ongoing Balancing....3052
Storage Migration Recommendations....3053
Create a Datastore Cluster....3053

Activate and Deactivate Storage DRS ... 3053
Set the Automation Level for Datastore Clusters ... 3054
Setting the Aggressiveness Level for Storage DRS ... 3054
Set Storage DRS Runtime Rules ... 3055
Datastore Cluster Requirements ... 3055
Adding and Removing Datastores from a Datastore Cluster ... 3056
Using Datastore Clusters to Manage Storage Resources ... 3056
Using Storage DRS Maintenance Mode ... 3056
Applying Storage DRS Recommendations ... 3057
Change Storage DRS Automation Level for a Virtual Machine ... 3058
Set Up Off-Hours Scheduling for Storage DRS ... 3059
Storage DRS Anti-Affinity Rules ... 3059
Clear Storage DRS Statistics ... 3062
Storage vMotion Compatibility with Datastore Clusters ... 3063
Using NUMA Systems with ESXi ... 3063
What is NUMA? ... 3063
Challenges for Operating Systems ... 3064
How ESXi NUMA Scheduling Works ... 3064
VMware NUMA Optimization Algorithms and Settings ... 3065
Home Nodes and Initial Placement ... 3065
Dynamic Load Balancing and Page Migration ... 3065
Transparent Page Sharing Optimized for NUMA ... 3066
Resource Management in NUMA Architectures ... 3066
Using Virtual NUMA ... 3066
Virtual NUMA Controls ... 3067
Specifying NUMA Controls ... 3067
Associate Virtual Machines with Specific Processors ... 3068
Associate Memory Allocations with Specific NUMA Nodes Using Memory Affinity ... 3068
Associate Virtual Machines with Specified NUMA Nodes ... 3069
Advanced Attributes ... 3069
Set Advanced Host Attributes ... 3070
Advanced Memory Attributes ... 3070
Advanced NUMA Attributes ... 3071
Set Advanced Virtual Machine Attributes ... 3072
Advanced Virtual Machine Attributes ... 3072
Advanced Virtual NUMA Attributes ... 3073
Latency Sensitivity ... 3074
Adjust Latency Sensitivity ... 3074
About Reliable Memory ... 3075
View Reliable Memory ... 3075

Backing Guest vRAM with 1GB Pages ... 3075
Fault Definitions ... 3076
Virtual Machine is Pinned ... 3076
Virtual Machine not Compatible with any Host ... 3076
VM/VM DRS Rule Violated when Moving to another Host ... 3076
Host Incompatible with Virtual Machine ... 3076
Host Has Virtual Machine That Violates VM/VM DRS Rules ... 3076
Host has Insufficient Capacity for Virtual Machine ... 3076
Host in Incorrect State ... 3077
Host Has Insufficient Number of Physical CPUs for Virtual Machine ... 3077
Host has Insufficient Capacity for Each Virtual Machine CPU ... 3077
The Virtual Machine Is in vMotion ... 3077
No Active Host in Cluster ... 3077
Insufficient Resources ... 3077
Insufficient Resources to Satisfy Configured Failover Level for HA ... 3077
No Compatible Hard Affinity Host ... 3077
No Compatible Soft Affinity Host ... 3077
Soft Rule Violation Correction Disallowed ... 3077
Soft Rule Violation Correction Impact ... 3078
DRS Troubleshooting Information ... 3078
Cluster Problems ... 3078
Load Imbalance on Cluster ... 3078
Cluster is Yellow ... 3078
Cluster is Red Because of Inconsistent Resource Pool ... 3078
Cluster Is Red Because Failover Capacity Is Violated ... 3079
No Hosts are Powered Off When Total Cluster Load is Low ... 3079
Hosts Are Powered-off When Total Cluster Load Is High ... 3079
DRS Seldom or Never Performs vMotion Migrations ... 3079
Host Problems ... 3080
DRS Recommends Host Be Powered on to Increase Capacity When Total Cluster Load Is Low ... 3080
Total Cluster Load Is High ... 3080
Total Cluster Load Is Low ... 3081
DRS Does Not Evacuate a Host Requested to Enter Maintenance or Standby Mode ... 3081
DRS Does Not Move Any Virtual Machines onto a Host ... 3081
DRS Does Not Move Any Virtual Machines from a Host ... 3081
Virtual Machine Problems ... 3082
Insufficient CPU or Memory Resources ... 3082
VM/VM DRS Rule or VM/Host DRS Rule Violated ... 3083
Virtual Machine Power On Operation Fails ... 3083
DRS Does Not Move the Virtual Machine ... 3083

vSphere Availability 3085

Business Continuity and Minimizing Downtime 3085

Reducing Planned Downtime 3085

Preventing Unplanned Downtime 3085

vSphere HA Provides Rapid Recovery from Outages 3086

vSphere Fault Tolerance Provides Continuous Availability 3087

Protecting vCenter Server with vCenter High Availability 3087

Protecting vCenter Server with VMware Service Lifecycle Manager 3087

Creating and Using vSphere HA Clusters 3087

How vSphere HA Works 3088

Primary and Secondary Hosts 3088

Host Failure Types 3089

Determining Responses to Host Issues 3089

VM and Application Monitoring 3091

VM Component Protection 3092

Network Partitions 3093

Datastore Heartbeating 3093

vSphere HA Security 3094

vSphere HA Admission Control 3095

Cluster Resources Percentage Admission Control 3095

Slot Policy Admission Control 3097

Dedicated Failover Hosts Admission Control 3099

vSphere HA Interoperability 3100

Using vSphere HA with vSAN 3100

Using vSphere HA and DRS Together 3101

Other vSphere HA Interoperability Issues 3102

Creating a vSphere HA Cluster 3103

vSphere HA Checklist 3103

Create a vSphere HA Cluster in the vSphere Client 3104

Configuring vSphere Availability Settings 3104

Configuring Responses to Failures 3105

Configure Proactive HA 3107

Configure Admission Control 3108

Configure Heartbeat Datastores 3109

Set Advanced Options 3109

Best Practices for VMware vSphere® High Availability Clusters 3112

Best Practices for Networking 3112

Best Practices for Interoperability 3114

Best Practices for Cluster Monitoring 3115

Change in behavior for HA VIBs 3115

Providing Fault Tolerance for Virtual Machines 3115
How Fault Tolerance Works 3115
Fault Tolerance Use Cases 3116
Fault Tolerance Requirements, Limits, and Licensing 3116
Fault Tolerance Interoperability 3117
vSphere Features not Supported with Fault Tolerance 3117
Features and Devices Incompatible with Fault Tolerance 3118
Using Fault Tolerance with DRS 3118
Preparing Your Cluster and Hosts for Fault Tolerance 3118
Fault Tolerance Checklist 3119
Configure Networking for Host Machines 3120
Create Cluster and Check Compliance 3120
Using Fault Tolerance 3120
Validation Checks for Turning On Fault Tolerance 3121
Turn On Fault Tolerance 3122
Turn Off Fault Tolerance 3122
Suspend Fault Tolerance 3123
Migrate Secondary 3123
Test Failover 3123
Test Restart Secondary 3123
Upgrade Hosts Used for Fault Tolerance 3124
Activate Fault Tolerance Encryption 3124
Best Practices for Fault Tolerance 3125
Legacy Fault Tolerance 3126
Troubleshooting Fault Tolerant Virtual Machines 3126
Hardware Virtualization Not Enabled 3127
Compatible Hosts Not Available for Secondary VM 3127
Secondary VM on Overcommitted Host Degrades Performance of Primary VM 3127
Increased Network Latency Observed in FT Virtual Machines 3128
Some Hosts Are Overloaded with FT Virtual Machines 3128
Losing Access to FT Metadata Datastore 3128
Turning On vSphere FT for Powered-On VM Fails 3129
FT Virtual Machines not Placed or Evacuated by vSphere DRS 3129
Fault Tolerant Virtual Machine Failovers 3129
vCenter High Availability 3130
Plan the vCenter HA Deployment 3130
vCenter Architecture Overview 3130
vCenter HA Hardware and Software Requirements 3131
vCenter HA Configuration Workflow 3132
Configure the Network 3133

Configure vCenter HA With the vSphere Client....3133
Manage the vCenter HA Configuration....3135
Set Up SNMP Traps....3135
Set Up Your Environment to Use Custom Certificates....3136
Manage vCenter HA SSH Keys....3136
Initiate a vCenter HA Failover....3137
Edit the vCenter HA Cluster Configuration....3137
Perform Backup and Restore Operations....3138
Remove a vCenter HA Configuration....3139
Reboot All vCenter HA Nodes....3139
Change the Server Environment....3139
Collecting Support Bundles for a vCenter HA Node....3139
Troubleshoot Your vCenter HA Environment....3140
vCenter HA Clone Operation Fails During Deployment....3140
Redeploy the Passive or Witness node....3140
vCenter HA Deployment Fails with an Error....3141
Troubleshooting a Degraded vCenter HA Cluster....3141
Recovering from Isolated vCenter HA Nodes....3142
Resolving Failover Failures....3142
VMware vCenter® HA Alarms and Events....3143
Patching a vCenter High Availability Environment....3144
vSphere Monitoring and Performance....3145
Updated Information....3145
Monitoring Inventory Objects with Performance Charts....3145
Performance Chart Types....3146
Data Counters....3146
Metric Groups in vSphere....3149
Data Collection Intervals....3149
Data Collection Levels....3150
View Performance Charts....3151
Performance Charts Options Available Under the View Menu....3151
Overview Performance Charts....3152
Clusters....3152
Data centers....3161
Datastores and Datastore Clusters....3164
Hosts....3174
Resource Pools....3199
vApps....3205
Virtual Machines....3209
Working with Advanced and Custom Charts....3235

View Advanced Performance Charts in the vSphere Client....3235
Change Advanced Chart Settings....3236
Create a Custom Advanced Chart....3236
Delete a Custom Advanced Chart View....3237
Save Chart Data to a File....3237
Troubleshoot and Enhance Performance....3237
Solutions for Consistently High CPU Usage....3238
Solutions for Memory Performance Problems....3238
Solutions for Storage Performance Problems....3239
Solutions for Disk Performance Problems....3239
Solutions for Poor Network Performance....3240
Empty Performance Charts....3241
Solutions for Performance Issues With Memory Mode....3242
Monitoring Guest Operating System Performance....3242
Enable Statistics Collection for Guest Operating System Performance Analysis....3243
View Performance Statistics for Windows Guest Operating Systems....3243
Monitoring Host Health Status....3243
Monitor Hardware Health Status in the vSphere Client....3244
Monitoring and Diagnostics of vSphere Health....3244
Check health of the system using Skyline Health for vSphere....3244
Analyse issues using VMware Skyline Health Diagnostics tool....3245
Monitoring Events, Alarms, and Automated Actions....3246
View Events in vSphere Client....3247
Export Events in vSphere Client....3248
View System Event Log....3248
Export System Event Log Data....3248
Consolidate Identical Events....3248
Configure Events Burst Filter....3249
Streaming Events to a Remote Syslog Server....3250
Forward vCenter Server Log Files to Remote Syslog Server....3251
Configure Streaming of Events to a Remote Syslog Server....3252
Retention of Events in the vCenter Server Database....3252
Configure Database Settings....3253
View Triggered Alarms....3253
Live Refresh of Recent Tasks and Alarms....3253
Set an Alarm in the vSphere Client....3254
Create or Edit Alarms....3254
Specify Alarm Name, Description, and Target....3254
Specify Alarm Rules....3254
Specify Alarm Reset Rules....3256

Review and Enable Alarm....3257
Disable Alarms on Specific Objects....3258
Acknowledge Triggered Alarms....3258
Reset Triggered Event Alarms....3258
Monitoring Solutions with the vCenter Solutions Manager....3259
View Solutions....3259
vSphere ESX Agent Manager....3260
Monitor ESX Agent Health Status....3260
Resolve Agency Issues....3260
Monitoring the Health of Services and Nodes....3261
View the Health Status of Nodes....3261
View the Health Status of Services....3262
Performance Monitoring Utilities: resxtop and esxtop....3262
Using the esxtop Utility....3262
Using the resxtop Utility....3263
Using esxtop or resxtop in Interactive Mode....3264
Interactive Mode Command-Line Options....3264
CPU Panel....3266
CPU Power Panel....3269
Memory Panel....3270
Storage Adapter Panel....3273
Storage Device Panel....3274
Virtual Machine Storage Panel....3276
Network Panel....3277
Interrupt Panel....3278
Using Batch Mode....3279
Prepare for Batch Mode....3279
Use esxtop or resxtop in Batch Mode....3279
Batch Mode Command-Line Options....3279
Using Replay Mode....3280
Prepare for Replay Mode....3280
Use esxtop in Replay Mode....3280
Replay Mode Command-Line Options....3281
Using the vimtop Plug-In to Monitor the Resource Use of Services....3281
Monitor Services By Using vimtop in Interactive Mode....3281
Interactive Mode Command-Line Options....3281
Interactive Mode Single-Key Commands for vimtop....3282
Monitoring Networked Devices with SNMP and vSphere....3283
Using SNMP Traps with vCenter Server....3284
Configure SNMP Settings for vCenter Server....3284

Configure SNMP for ESXi....3285
Configure the SNMP Agent for Polling....3285
Configure ESXi for SNMPv1 and SNMPv2c....3285
Configure ESXi for SNMP v3....3287
Configure the Source of Hardware Events Received by the SNMP Agent....3290
Configure the SNMP Agent to Filter Notifications....3290
Configure SNMP Management Client Software....3291
SNMP Diagnostics....3291
Monitor Guest Operating Systems with SNMP....3292
VMware MIB Files....3292
SNMPv2 Diagnostic Counters....3293
System Log Files....3294
View System Logs on an ESXi Host....3295
System Logs....3295
ESXi System Logs....3295
vSphere Client Logs....3295
Export System Log Files....3296
ESXi Log Files....3296
Upload Logs Package to a VMware Service Request....3297
Configure Syslog on ESXi Hosts....3297
Configuring Logging Levels for the Guest Operating System....3297
Change the Number of Virtual Machine Log Files....3298
Control When to Switch to New Virtual Machine Log Files....3298
Collecting Log Files....3299
Set Verbose Logging....3299
Collect vSphere Log Files....3299
Collect ESXi Log Files....3300
ESXi Log File Locations....3300
Configure Log Filtering on ESXi Hosts....3301
Turn Off Compression for vpxd Log Files....3302
ESXi VMkernel Files....3302
vSphere Single Host Management - VMware Host Client....3303
Updated Information....3303
VMware Host Client Overview....3304
VMware Host Client System Requirements....3304
Using the VMware Host Client....3304
Start the VMware Host Client and Log In....3305
Log Out of the VMware Host Client....3305
Configuring Customer Experience Improvement Program....3305
Host Management with the VMware Host Client....3306

Managing System Settings in the VMware Host Client....3306
Manage Advanced Settings in the VMware Host Client....3306
Create an Initial Welcome Message for the Direct Console User Interface and the VMware Host Client....3306
Configure the VMware Host Client User Interface Session Timeout....3307
Configure the SOAP Session Timeout in the VMware Host Client....3308
Configure the Passwords and Account Lockout Policy in the VMware Host Client....3308
Configure Syslog in theVMware Host Client....3312
Configure Advanced TLS/SSL Key Options....3312
Configure Userworld Memory Zeroing....3313
Change Autostart Configuration in theVMware Host Client....3314
Edit the Time Configuration of anESXi Host in theVMware Host Client....3315
Managing Hardware for an ESXi Host by Using the VMware Host Client....3316
Host Power Management Policies....3316
Change Power Management Policies in the VMware Host Client....3316
Change the Hardware Label in the VMware Host Client....3317
Licensing for ESXi Hosts....3317
View Licensing Information About the VMware Host Client Environment....3318
Assign a License Key to an ESXi Host in the VMware Host Client....3318
Remove a License from an ESXi Host in the VMware Host Client....3319
Manage Services in the VMware Host Client....3319
Managing Security and Users for an ESXi Host by Using the VMware Host Client....3319
Managing Host Authentication by Using the VMware Host Client....3319
Managing Host Certificates by Using the VMware Host Client....3321
Managing Users with the VMware Host Client....3322
Managing ESXi Roles in the VMware Host Client....3323
Managing Hosts in vCenter Server....3324
Update Your VMware Host Client Environment to the Latest Version....3325
Unable to Connect from the VMware Host Client to an ESXi Host After Upgrading to a Newer Version of ESXi....3325
Switch to the vSphere Client....3326
Disconnect an ESXi Host from vCenter Server by Using the VMware Host Client....3326
Reboot or Shut Down an ESXi Host in the VMware Host Client....3326
Using the ESXi Shell....3327
Enable the Secure Shell (SSH) in the VMware Host Client....3327
Enable the ESXi Console Shell in the VMware Host Client....3327
Create a Timeout for ESXi Shell Availability in the VMware Host Client....3328
Create a Timeout for Idle ESXi Shell Sessions in the VMware Host Client....3328
Place a Host in Maintenance Mode in the VMware Host Client....3328
Managing Permissions in the VMware Host Client....3329
Permission Validation....3329

Assign Permissions to a User for an ESXi Host in the VMware Host Client ... 3330
Remove Permissions for a User in the VMware Host Client ... 3330
Assign a User Permissions for a Virtual Machine in the VMware Host Client ... 3330
Remove Permissions for a Virtual Machine in the VMware Host Client ... 3331
Generate a Support Bundle in the VMware Host Client ... 3331
Lockdown Mode ... 3332
Put an ESXi Host in Normal Lockdown Mode by Using the VMware Host Client ... 3332
Put an ESXi Host in Strict Lockdown Mode by Using the VMware Host Client ... 3333
Exit Lockdown Mode by Using the VMware Host Client ... 3333
Specify Lockdown Mode Exception Users in the VMware Host Client ... 3333
Administering CPU Resources by Using the VMware Host Client ... 3333
View Processor Information by Using the VMware Host Client ... 3333
Assign a Virtual Machine to a Specific Processor in the VMware Host Client ... 3334
Monitoring an ESXi Host in the VMware Host Client ... 3334
View Charts in the VMware Host Client ... 3334
Monitor Hardware Health Status in the VMware Host Client ... 3334
View Events in the VMware Host Client ... 3334
View Tasks in the VMware Host Client ... 3335
View System Logs in the VMware Host Client ... 3335
View Notifications in the VMware Host Client ... 3336
Virtual Machine Management with the VMware Host Client ... 3336
Create a Virtual Machine in the VMware Host Client ... 3336
Deploying a Virtual Machine from an OVF or OVA File in the VMware Host Client ... 3339
OVF and OVA Limitations for the VMware Host Client ... 3339
Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client ... 3340
Register an Existing Virtual Machine in the VMware Host Client ... 3341
Using Consoles in the VMware Host Client ... 3341
Install the VMware Remote Console Application in the VMware Host Client ... 3342
Launch Remote Console for a Virtual Machine in the VMware Host Client ... 3342
Open a Virtual Machine Console in the VMware Host Client ... 3342
Managing a Guest Operating System in the VMware Host Client ... 3342
Shut Down or Restart a Guest Operating System by Using the VMware Host Client ... 3342
Change the Guest Operating System in the VMware Host Client ... 3342
Introduction to VMware Tools ... 3343
Configuring a Virtual Machine in the VMware Host Client ... 3345
Check the Virtual Machine Compatibility in the VMware Host Client ... 3345
Change the Name of a Virtual Machine in the VMware Host Client ... 3345
View the Location of the Virtual Machine Configuration File in the VMware Host Client ... 3345
Configure the Virtual Machine Power States in theVMware Host Client ... 3346
Edit the Configuration File Parameters in the VMware Host Client ... 3347

Configure Autostart Options for a Virtual Machine in the VMware Host Client ... 3348
Upgrade Virtual Machine Compatibility by Using the VMware Host Client ... 3348
Virtual CPU Configuration ... 3349
Virtual Memory Configuration ... 3351
Network Virtual Machine Configuration ... 3354
Virtual Disk Configuration ... 3357
Virtual Machine Controller Configuration in the VMware Host Client ... 3363
Other Virtual Machine Device Configuration in the VMware Host Client ... 3367
Securing Virtual Machines with Intel Software Guard Extensions ... 3373
Managing Virtual Machines in the VMware Host Client ... 3374
Access a Virtual Machine in the VMware Host Client ... 3374
Power States of a Virtual Machine in the VMware Host Client ... 3375
Use Virtual Machine Column Configuration in the VMware Host Client ... 3375
Remove Virtual Machines from a Host in the VMware Host Client ... 3375
Remove Virtual Machines from a Datastore in the VMware Host Client ... 3376
Register a Virtual Machine in the VMware Host Client ... 3376
Using Snapshots To Manage Virtual Machines ... 3376
Monitoring a Virtual Machine in the VMware Host Client ... 3384
View Virtual Machine Performance Charts in the VMware Host Client ... 3384
View Virtual Machine Events in the VMware Host Client ... 3384
View Virtual Machine Tasks in the VMware Host Client ... 3385
View Virtual Machine Log Browser in the VMware Host Client ... 3385
View Virtual Machine Notifications in the VMware Host Client ... 3385
Securing Virtual Machines in the VMware Host Client ... 3385
Remove a vTPM device from a VM in the VMware Host Client ... 3386
Enable or Disable Virtualization-based Security on an Existing VM in the VMware Host Client ... 3387
Managing Storage in the VMware Host Client ... 3387
Working with Datastores in the VMware Host Client ... 3387
View Datastore Information in the VMware Host Client ... 3388
Create a VMFS Datastore in theVMware Host Client ... 3388
Increasing VMFS Datastore Capacity ... 3388
Mounting a Network File System Datastore in the VMware Host Client ... 3389
Unmount a Datastore in the VMware Host Client ... 3390
Using Datastore File Browser in the VMware Host Client ... 3391
Rename a Datastore in the VMware Host Client ... 3394
Delete a VMFS Datastore in the VMware Host Client ... 3394
Storage Thin Provisioning in the VMware Host Client ... 3394
Managing Storage Adapters in the VMware Host Client ... 3395
View Storage Adapters in the VMware Host Client ... 3396
Configuring Software iSCSI Adapters in the VMware Host Client ... 3396

Managing Storage Devices in the VMware Host Client ... 3404
View Storage Devices in the VMware Host Client ... 3404
Clear a Device Partition Table in theVMware Host Client ... 3404
Edit Individual Device Partitions in theVMware Host Client ... 3405
Managing Persistent Memory ... 3405
Modes of Consumption of the Persistent Memory Resources of the Host ... 3405
Structure of the PMem Datastore ... 3406
Monitoring Storage in the VMware Host Client ... 3407
Monitor Datastores in the VMware Host Client ... 3408
Monitoring vSAN in the VMware Host Client ... 3408
Performing Storage Refresh and Rescan Operations in the VMware Host Client ... 3412
Perform Adapter Rescan in the VMware Host Client ... 3412
Perform Device Rescan in the VMware Host Client ... 3412
Change the Number of Scanned Storage Devices in the VMware Host Client ... 3412
Networking in the VMware Host Client ... 3413
Managing Port Groups in the VMware Host Client ... 3413
View Port Group Information in the VMware Host Client ... 3413
Add a Virtual Switch Port Group in the VMware Host Client ... 3413
Edit Port Group Settings in theVMware Host Client ... 3414
Remove a Virtual Switch Port Group in the VMware Host Client ... 3417
Managing Virtual Switches in the VMware Host Client ... 3417
View Virtual Switch Information in the VMware Host Client ... 3417
Add a Standard Virtual Switch in theVMware Host Client ... 3417
Remove a Standard Virtual Switch in the VMware Host Client ... 3419
Add a Physical Uplink to a Virtual Switch in the VMware Host Client ... 3419
Edit Virtual Switch Settings in theVMware Host Client ... 3419
Managing Physical Network Adapters in the VMware Host Client ... 3422
View Physical Network Adapter Information in the VMware Host Client ... 3422
Edit Physical NICs in the VMware Host Client ... 3422
Managing VMkernel Network Adapters in the VMware Host Client ... 3422
View VMkernel Network Adapter Information in the VMware Host Client ... 3423
Add a VMkernel Network Adapter in theVMware Host Client ... 3423
Edit VMkernel Network Adapter Settings in theVMware Host Client ... 3424
Remove a VMkernel Network Adapter in the VMware Host Client ... 3425
View TCP/IP Stack Configuration on a Host in the VMware Host Client ... 3425
Change the Configuration of a TCP/IP Stack on a Host in theVMware Host Client ... 3425
Configuring ESXi Firewall in the VMware Host Client ... 3426
Manage ESXi Firewall Settings by Using the VMware Host Client ... 3426
Add Allowed IP Addresses for an ESXi Host by Using the VMware Host Client ... 3426
Monitoring Networking Events and Tasks in the VMware Host Client ... 3426

Monitor Port Groups in the VMware Host Client....3427
Monitor Virtual Switches in the VMware Host Client....3427
Monitor Physical Network Adapters in the VMware Host Client....3427
Monitor VMkernel Network Adapters in the VMware Host Client....3427
Monitor TCP/IP Stacks in the VMware Host Client....3428
Setup for Windows Server Failover Clustering on VMware vSphere....3429
Getting Started with WSFC on VMware® vSphere®....3429
Clustering Configuration Overview....3429
Hosting virtual nodes of a WSFC on a Single Host....3430
Clustering Virtual Machines Across Physical Hosts....3430
Clustering Physical Machines with Virtual Machines....3431
Hardware and Software Requirements for WSFC on vSphere....3432
Supported Shared Storage Configurations....3433
Round Robin Path Selection Policy (PSP_RR) Support for disk resources used by WSFC....3434
iSCSI Support for WSFC....3434
FCoE Support for WSFC....3435
vMotion support for WSFC....3435
VMware vSphere® Virtual Volumes™ Support for WSFC....3436
vSphere WSFC Setup Limitations....3436
WSFC and Booting from a SAN....3437
Cluster Virtual Machines Across Physical ESXi Hosts....3437
Clustered VMDK support for WSFC....3437
Activating Clustered VMDK Support....3437
Configuration Maximums for Clustered VMDK Support....3438
Recommendations for using Clustered VMDKs with WSFC....3438
Requirements for using Clustered VMDKs with WSFC....3438
Limitations of Clustered VMDK support for WSFC....3439
Create the First Node for WSFC Clusters Across Physical Hosts....3439
Create Additional Nodes for a WSFC Across Physical Hosts....3440
Add Hard Disks to the First VM, first node of a WSFC, for Clusters Across Physical Hosts with pRDMs....3440
Add Hard Disks to the First Node of a WSFC Across Physical Hosts with vVols....3441
Add Hard Disks to First Node for Cluster Across Physical Hosts with Clustered VMDKs on VMFS....3442
Add Hard Disks to Additional Nodes for Clusters Across Physical Hosts....3442
Use WSFC in an vSphere HA and vSphere DRS Environment....3443
Enable vSphere HA and vSphere DRS in ESXi....3443
Create VM-VM Affinity Rules for WSFC Virtual Machines....3443
Set DRS Automation Level for WSFC Virtual Machines....3444
Using vSphere DRS Groups and VM-Host Affinity Rules with WSFC Virtual Machines....3444
Create a Virtual Machine DRS Group (WSFC)....3445
Create a Host DRS Group (WSFC)....3445

Set up VM-Host Affinity Rules for DRS Groups (WSFC)....3446
vSphere WSFC Setup Checklist....3446
Cluster Virtual Machines on One Physical Host....3448
Create the First Node of a WSFC on One Physical ESXi Host....3449
Create Additional Nodes for Clusters on One Physical Host....3449
Add Hard Disks to the First Node for Clusters on One Physical Host....3450
Add Hard Disks to Additional Nodes for Clusters on One Physical Host....3450
Cluster Physical and Virtual Machines....3451
Create the First Node for a Cluster of Physical and Virtual Machines....3451
Create the Second Node for a Cluster of Physical and Virtual Machines....3451
Add Hard Disks to the Second Node for a Cluster of Physical and Virtual Machines....3452
Install Microsoft Cluster Service....3453
Create Additional Physical-Virtual Pairs....3453
Documentation Legal Notice....3454

Release Notes

Release notes include product enhancements and notices, bug fixes, and resolved issues.

VMware vSphere 7.0 Release Notes

This document contains the following sections

- Introduction
- What's New
- Internationalization
- Compatibility
- Before You Begin
- Installation and Upgrades for This Release
- Open Source Components for vSphere 7.0
- Product Support Notices
- Known Issues

Introduction

ESXi 7.0 | 2 APR 2020 | ISO Build 15843807 vCenter Server 7.0 | 2 APR 2020 | ISO Build 15952498 Check for additions and updates to these release notes.

What's New

- This release of VMware vSphere 7.0 includes VMware ESXi 7.0 and VMware vCenter Server 7.0. Read about the new and enhanced features in this release in What's New in vSphere 7.0.

Internationalization

vSphere 7.0 is available in the following languages:

- English
- French
- German
- Spanish
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

Components of vSphere 7.0, including vCenter Server, ESXi, the vSphere Client, and the vSphere Host Client, do not accept non-ASCII input.

Compatibility

ESXi and vCenter Server Version Compatibility

The VMware Product Interoperability Matrix provides details about the compatibility of current and earlier versions of VMware vSphere components, including ESXi, VMware vCenter Server, and optional VMware products. Check the VMware Product Interoperability Matrix also for information about supported management and backup agents before you install ESXi or vCenter Server.

The vSphere Lifecycle Manager and vSphere Client are packaged with vCenter Server.

Hardware Compatibility for ESXi

To view a list of processors, storage devices, SAN arrays, and I/O devices that are compatible with vSphere 7.0, use the ESXi 7.0 information in the VMware Compatibility Guide.

Device Compatibility for ESXi

To determine which devices are compatible with ESXi 7.0, use the ESXi 7.0 information in the VMware Compatibility Guide.

Guest Operating System Compatibility for ESXi

To determine which guest operating systems are compatible with vSphere 7.0, use the ESXi 7.0 information in the VMware Compatibility Guide.

Virtual Machine Compatibility for ESXi

Virtual machines that are compatible with ESX 3.x and later (hardware version 4) are supported with ESXi 7.0. Virtual machines that are compatible with ESX 2.x and later (hardware version 3) are not supported. To use such virtual machines on ESXi 7.0, upgrade the virtual machine compatibility. See the *ESXi Upgrade* documentation.

Before You Begin

vSphere 7.0 requires one CPU license for up to 32 physical cores. If a CPU has more than 32 cores, additional CPU licenses are required as announced in "Update to VMware's per-CPU Pricing Model". Prior to upgrading ESXi hosts, you can determine the number of licenses required using the license counting tool described in "Counting CPU licenses needed under new VMware licensing policy".

Installation and Upgrades for This Release

Installation Notes for This Release

Read the *ESXi Installation and Setup* and the vCenter Server Installation and Setupdocumentation for guidance about installing and configuring ESXi and vCenter Server.

Although the installations are straightforward, several subsequent configuration steps are essential. Read the following documentation:

- "License Management" in the *vCenter Server and Host Management* documentation
- "Networking" in the *vSphere Networking* documentation
- "Security" in the *vSphere Security* documentation for information on firewall ports

VMware's Configuration Maximums tool helps you plan your vSphere deployments. Use this tool to view the limits for virtual machines, ESXi, vCenter Server, vSAN, networking, and so on. You can also compare limits for two or more product releases. The VMware Configuration Maximums tool is best viewed on larger format devices such as desktops and laptops.

VMware Tools Bundling Changes in ESXi 7.0

In ESXi 7.0, a subset of VMware Tools 11.0.5 and VMware Tools 10.3.21 ISO images are bundled with the ESXi 7.0 host.

The following VMware Tools 11.0.5 ISO image is bundled with ESXi:

- windows.iso: VMware Tools image for Windows Vista or higher

The following VMware Tools 10.3.21 ISO image is bundled with ESXi:

- linux.iso: VMware Tools image for Linux OS with glibc 2.5 or higher

The following VMware Tools 11.0.5 ISO images are available for download:

- darwin.iso: VMware Tools image for OSX

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- VMware Tools 11.0.5 Release Notes
- VMware Tools 10.3.21 Release Notes
- VMware Tools Documentation

Migrating Third-Party Solutions

For information about upgrading with third-party customizations, see the *ESXi Upgrade* documentation. For information about using Image Builder to make a custom ISO, see the *ESXi Installation and Setup* documentation.

Upgrades and Installations Disallowed for Unsupported CPUs

Comparing the processors supported by vSphere 6.7, vSphere 7.0 no longer supports the following processors:

- Intel Family 6, Model = 2C (Westmere-EP)
- Intel Family 6, Model = 2F (Westmere-EX)

During an installation or upgrade, the installer checks the compatibility of the host CPU with vSphere 7.0. If your host hardware is not compatible, a purple screen appears with an incompatibility information message, and the vSphere 7.0 installation process stops.

The following CPUs are supported in the vSphere 7.0 release, but they may not be supported in future vSphere releases. Please plan accordingly:

- Intel Family 6, Model = 2A (Sandy Bridge DT/EN, GA 2011)
- Intel Family 6, Model = 2D (Sandy Bridge EP, GA 2012)
- Intel Family 6, Model = 3A (Ivy Bridge DT/EN, GA 2012)
- AMD Family 0x15, Model = 01 (Bulldozer, GA 2012)

Upgrade Notes for This Release

For instructions about upgrading ESXi hosts and vCenter Server, see the *ESXi Upgrade* and the vCenter Server Upgradedocumentation.

Open Source Components for vSphere 7.0

The copyright statements and licenses applicable to the open source software components distributed in vSphere 7.0 are available at http://www.vmware.com. You need to log in to your My VMware account. Then, from the **Downloads** menu, select **vSphere**. On the **Open Source** tab, you can also download the source files for any GPL, LGPL, or other similar licenses that require the source code or modifications to source code to be made available for the most recent available release of vSphere.

Product Support Notices

- VMware vSphere Clients

  In vSphere 7.0, you can take advantage of the features available in the vSphere Client (HTML5). The Flash-based vSphere Web Client has been deprecated and is no longer available. For more information, see Goodbye, vSphere Web Client.

  The VMware Host Client is a web-based application that you can use to manage individual ESXi hosts that are not connected to a vCenter Server system.

- VMware vSphere 7.0 and TLS Protocol

  In vSphere 7.0, TLS 1.2 is enabled by default. TLS 1.0 and TLS 1.1 are disabled by default. If you upgrade vCenter Server to 7.0 and that vCenter Server instance connects to ESXi hosts, other vCenter Server instances, or other services, you might encounter communication problems.

  To resolve this issue, you can use the TLS Configurator utility to enable older versions of the protocol temporarily on 7.0 systems. You can then disable the older less secure versions after all connections use TLS 1.2. For information, see Managing TLS Protocol Configuration with the TLS Configurator Utility.
- Removal of External Platform Services Controller

  In vSphere 7.0, deploying or upgrading vCenter Server in vSphere 7.0 requires the use of vCenter Server appliance, a preconfigured Linux virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller (PSC) services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All PSC services have been consolidated into vCenter Server, and deployment and administration have been simplified.
- Removal of vCenter Server for Windows Support

  In vSphere 7.0, vCenter Server for Windows has been removed and support is not available. For more information, see Farewell, vCenter Server for Windows.
- Removal of VNC Server from ESXi

  In vSphere 7.0, the ESXi built-in VNC server has been removed. Users will no longer be able to connect to a virtual machine using a VNC client by setting the **RemoteDisplay.vnc.enable** configure to be true. Instead, users should use the VM Console via the vSphere Client, the ESXi Host Client, or the VMware Remote Console, to connect virtual machines. Customers desiring VNC access to a VM should use the VirtualMachine.AcquireTicket("webmks") API, which offers a VNC-over-websocket connection. The webmks ticket offers authenticated access to the virtual machine console. For more information, please refer to the VMware HTML Console SDK Documentation.
- Deprecation of VMKLinux

  In vSphere 7.0, VMKLinux driver compatibility has been deprecated and removed. vSphere 7.0 will not contain support for VMKLinux APIs and associated VMKLinux drivers. Custom ISO will not be able to have any VMKLinux async drivers. All drivers contained in an ISO must be native drivers. All currently supported devices which are not supported by native drivers will not function and will not be recognized during installation or upgrade. VCG will not show any devices not supported by a native driver as supported in vSphere 7.0.
- Deprecation of 32-bit Userworld Support

  In vSphere 7.0, 32-bit userworld support has been deprecated. Userworlds are the components of ESXi used by partners to provide drivers, plugins, and other system extensions (distributed as VIBs). Userworlds are not customer accessible.

  vSphere 7.0 provides 64-bit userworld support through partner devkits and will retain 32-bit userworld support through this major release. Support for 32-bit userworlds will be permanently removed in the next major ESXi release. To avoid loss of functionality, customers should ensure any vendor-supplied VIBs in use are migrated to 64-bit before upgrading beyond the vSphere 7.0 release.
- Deprecation of Update Manager Plugin

  In vSphere 7.0, the Update Manager plugin used for administering vSphere Update Manager has been replaced with the Lifecycle Manager plugin. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plugin, along with new capabilities for vSphere Lifecycle Manager.
- Deprecation of Integrated Windows Authentication

  Integrated Windows Authentication (IWA) is deprecated in vSphere 7.0 and will be removed in a future release. For more information, see VMware Knowledge Base article 78506.
- Deprecation of DCUI Smart Card Authentication

  In a future vSphere release, support for Smart Card Authentication in DCUI will be discontinued. In place of accessing DCUI using Personal Identity Verification (PIV), Common Access Card (CAC), or SC650 smart card, users will be encouraged to perform operations through vCenter, PowerCLI, API calls, or by logging in with a username and password.

- Deprecation of Core Partition Profile in Host Profiles
  In vSphere 7.0, support for Coredump Partitions in Host Profiles has been deprecated. In place of Coredump Partitions, users should transition to Coredump Files.
- Deprecation of Software FCoE Adapters
  Starting from vSphere 7.0, VMware deprecates the configuration of software FCoE adapters that use the native FCoE stack in ESXi and plans to remove the feature in a future vSphere release.
- Vendor add-ons in MyVMware for use with vSphere Lifecycle Manager
  In vSphere 7.0, vendor add-ons are accessible through vCenter Server's vSphere Lifecycle Manager if the vCenter Server instance has been configured to use a proxy or Update Manager Download Service. To access add-ons from MyVMware, navigate to the **Custom ISOs and Add-ons** tab. Under the **OEM Customized Installer CDs and Add-ons**, you can find the custom add-ons from each of the vendors. For more information about vSphere Lifecycle Manager and vendor add-ons, see the Managing Host and Cluster Lifecycle documentation.

Known Issues

Installation, Upgrade, and Migration Issues

- **vmnic and vmhba device names change after an upgrade to ESXi 7.0**

On certain hardware platforms, vmnic and vmhba device names (aliases) might change across an upgrade to ESXi 7.0 from an earlier ESXi version. This occurs on systems whose firmware provides an ACPI _SUN method that returns a physical slot number of 0 for devices that are not in a pluggable slot.

Workaround: You can rename devices by using the instructions in VMware knowledge base article 2091560.

- **The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"**

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

- **Problems upgrading to vSphere 7.0 with pre-existing CIM providers**

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency. The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

- **Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0**

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

- **Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error**

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error install.vmafd.vmdir_vdcpromo_error_21, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

- **Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service**

If the vSphere Authentication Proxy service (vmcam) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or disable different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the vmcam port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

- **Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade**

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

- **Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message**

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message IP already exists in the network. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: /var/log/vmware/upgrade/UpgradeRunner.log

Workaround:

- a. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
  b. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

- **When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect**

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the max_vfs module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the max_vfs module parameter and reboot the ESXi host.

- **Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance**

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of DVS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

- **After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance**

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

- **Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails**

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

- **After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail**

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

- a. Remove any duplicate claim rules of the system default rules from the Host Profile document.
  b. Check the compliance status.
  c. Remediate the host.
  d. If the previous steps do not help, reboot the host.

- **Error message displays in the vCenter Server Management Interface**

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

- **Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host**

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

- **Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host**

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

- **Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client**

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

- **Reduced throughput in networking performance on Intel 82599/X540/X550 NICs**

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben

After running the command, reboot.

- **High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled**

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the ethernetx.ctxPerDev setting to enable multiple worlds.

- **IPv6 traffic fails to pass through VMkernel ports using IPsec**

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

- **Higher ESX network performance with a portion of CPU usage increase**

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

esxcli network ip interface remove --interface-name=vmk1

esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1

- **VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion**

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

- **Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance**

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

- a. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
  b. Log in to the VCSA using ssh. Execute the following script:

./opt/vmware/share/vami/vami_config_net

Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:

./opt/likewise/bin/lw-update-dns

Restart all the services on the VCSA to update the IP information on the DNS server.

- **It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.**

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

- **Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.**

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of hostd using the following command.

localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path host/vim/vmvisor/hostd --units mb --min 2048 --max 2048

Note that this will cause hostd to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

- **DRS may incorrectly launch vMotion if the network reservation is configured on a VM**

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- – The VM connects to an NSX logical switch configured with a network reservation.
  – Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

- **When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."**

- – For stateless ESXi on Distributed Virtual Switch (DVS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
  – For stateful ESXi on DVS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same DVS.

- **Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail**

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

esxcfg-module

- **New vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS**

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

- **VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers**

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

- **Setting the loglevel for nvme_pcie driver fails with an error**

When you set the loglevel for nvme_pcie driver with the command esxcli nvme driver loglevel set -l <*log level*>, the action fails with the error message:

Failed to set log level 0x2.

This command was retained for compatibility consideration with NVMe driver, but it is not supported for nvme_pcie driver.

Workaround: None. This condition will exist when the nvme_pcie feature is enabled.

- **ESXi might terminate I/O to NVMeOF devices due to errors on all active paths**

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

- **VOMA check on NVMe based VMFS datastores fails with error**

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

ERROR: Failed to reserve device. Function not implemented

Example:

voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>

Running VMFS Checker version 2.1 in check mode

Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity

Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).

ERROR: Failed to reserve device. Function not implemented

Aborting VMFS volume check

VOMA failed to check device : General Error

Workaround: None. If you need to analyse VMFS metadata, collect it using the -l option, and pass to VMware customer support. The command for collecting the dump is:

voma -l -f dump -d /vmfs/devices/disks/:<partition#>

- **Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error**

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the VM reconfigure API might fail with the error message:

Cannot decrypt disk because key or password is incorrect.

Workaround: Use the attachDisk API rather than the VM reconfigure API to attach an encrypted FCD to an encrypted VM.

- **ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state**

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

- **After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible**

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple SCSI3 reservation conflict messages similar to the following:

2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219: SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340 (op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

vmkfstools -L registerkey /vmfs/devices/disks/<device name>

where the <device name> is the name of the device on which the datastore is created.

- **Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems**

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10 Windows Server 2016 Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

- **After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior**

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

- **A CNS query with the compliance status filter set might take unusually long time to complete**

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

- **New Deleted CNS volumes might temporarily appear as existing in the CNS UI**

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following: The object or item referred to could not be found.

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

- **New Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error**

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

- **New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client**

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

- **New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore**

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

- **Vendor providers go offline after a PNID change**

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

- **Cross vCenter migration of a virtual machine fails with an error**

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error The operation is not allowed in the current state.

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

- **Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB**

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path “runtime.hardwareStatusInfo.storageStatusInfo” as well.

Workaround: None.

- **vSphere UI host advanced settings shows the current product locker location as empty with an empty default**

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location symlink is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "esxcli system settings advanced remove -o ProductLockerLocation"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"

Run the following command to automatically figure out the location: export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker`

Add the setting: esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT

You can combine all the above steps in step 2 by issuing the single command:

esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s `readlink /productLocker`

- **Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.**

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

- **The postcustomization section of the customization script runs before the guest customization**

When you run the guest customization script for a Linux guest operating system, the precustomization section of the customization script that is defined in the customization specification runs before the guest customization and the postcustomization section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the postcustomization section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

- **Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error**

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.

Workaround: Retry the migration operation on the failed VMs one at a time.

- **Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error**

The URLs that contain an HTTP query parameter are not supported. For example, http://webaddress.com?file=abc.ovf or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

- **Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error**

When you import local .ovf files containing non-ASCII characters in their name, you might receive 400 Bad Request Error. When you use such .ovf files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive 400 Bad Request Error or 500 Internal Server Error.

Workaround:

- a. Remove the non-ASCII characters from the .ovf and .vmdk file names.
    - To edit the .ovf file, open it with a text editor.
    - Search the non-ASCII .vmdk file name and change it to ASCII.
  b. Import or deploy the saved files again.
- **New The third level of nested objects in a virtual machine folder is not visible**

Perform the following steps:

- a. Navigate to a data center and create a virtual machine folder.
  b. In the virtual machine folder, create a nested virtual machine folder.
  c. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

- **Modified VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD**

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- – All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
  – HA primary initiates failover due to APD on a host.
  – Power on API during HA failover fails due to one of the following:
    - APD across the same host
    - Cascading APD across the entire cluster
    - Storage issues
    - Resource unavailability
  – FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

- **You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively**

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

- **vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release**

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

- **ESXi 7.0 hosts cannot be added to a cluster that you manage with a single image by using vSphere Auto Deploy**

Attempting to add ESXi hosts to a cluster that you manage with a single image by using the "Add to Inventory" workflow in vSphere Auto Deploy fails. The failure occurs because no patterns are matched in an existing Auto Deploy ruleset. The task fails silently and the hosts remain in the Discovered Hosts tab.

Workaround:

- a. Remove the ESXi hosts that did not match the ruleset from the Discovered Hosts tab.
  b. Create a rule or edit an existing Auto Deploy rule, where the host target location is a cluster managed by an image.
  c. Reboot the hosts.

The hosts are added to the cluster that you manage by an image in vSphere Lifecycle Manager.

- **When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted**

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- – Configuring vSphere HA on a cluster fails.
  – Cannot complete the configuration of the vSphere HA agent on a host: Applying HA VIBs on the cluster encountered a failure.
  – Remediating vSphere HA fails: A general system error occurred: Failed to get Effective Component map.
  – Disabling vSphere HA fails: Delete Solution task failed. A general system error occurred: Cannot find hardware support package from depot or hardware support manager.

Workaround:

- – If the hardware support manager is temporarily unavailable, perform the following steps.
- a. Reconnect the hardware support manager to vCenter Server.
  b. Select a cluster from the Hosts and Cluster menu.
  c. Select the Configure tab.
  d. Under Services, click vSphere Availability.
  e. Re-enable vSphere HA.
- – If the hardware support manager is permanently unavailable, perform the following steps.
- a. Remove the hardware support manager and the hardware support package from the image specification
  b. Re-enable vSphere HA.
  c. Select a cluster from the Hosts and Cluster menu.
  d. Select the Updates tab.
  e. Click Edit .
  f. Remove the firmware and drivers addon and click Save.
  g. Select the Configure tab.
  h. Under Services, click vSphere Availability.
  i. Re-enable vSphere HA.

- **I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager**

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: iofilter XXX already exists. The iofilter remains listed as installed.

Workaround:

- a. Call IOFilter API UninstallIoFilter_Task from the vCenter Server managed object (IoFilterManager).
  b. Remediate the cluster in vSphere Lifecycle Manager.
  c. Call IOFilter API ResolveInstallationErrorsOnCluster_Task from the vCenter Server managed object (IoFilterManager) to update the database.

- **While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state**

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: Applying HA VIBs on the cluster encountered a failure.

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- – Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
  – Disable and re-enable vSphere HA for the cluster.

- **While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state**

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: Setting desired image spec for cluster failed.

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

- **Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters**

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

- **Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters**

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

- **Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager**

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message. The error message in English language: Virtual machine 'VMC on DELL EMC - FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx The error message in French language: La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx

Workaround: None.

- **Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image**

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

- **When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed**

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that vmware-fdm component will be removed.

Workaround: This message can be ignored. The conversion process installs the vmware-fdm component.

- **If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail**

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

- **When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails**

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

- a. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
  b. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

- **The Actions drop-down menu does not contain any items when your browser is set to language different from English**

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

- **Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on**

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"

reboot

- **RDMA traffic between two VMs on the same host might fail in PVRDMA environment**

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

- **Unreliable Datagram traffic QP limitations in qedrntv driver**

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are ibv_ud_pingpong and ib_send_bw.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

- **Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs**

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

- **ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment**

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: @BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19

Workaround: None.

- **ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers**

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

- **X710 or XL710 NICs might fail in ESXi**

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

- **NVMe-oF does not guarantee persistent VMHBA name after system reboot**

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

- **Backup fails for vCenter database size of 300 GB or greater**

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: Timeout! Failed to complete in 72000 seconds

Workaround: None.

- **Checking the compliance state of a ESXi 7.0 host against a host profile with version 6.5 or 6.7, results in an error for vmhba and vmrdma devices**

When checking the compliance of a ESXi 7.0 host that uses nmlx5_core or nvme_pcie driver against a host profile with version 6.5 or 6.7, you may observe the following errors, where address1 and address2 are specific to the affected system.

- – A vmhba device with bus type logical, address1 is not present on your host.
  – A vmrdma device with bus type logical, address2 is not present on your host.

The error is due to a mismatch between device addresses generated by the nmlx5_core or nvme_pcie driver in ESXi version 7.0 and earlier.

Workaround: The error may be ignored. The ESXi host functionality is unaffected. To resolve the compliance state error, re-extract the host profile from a ESXi host version 7.0, and apply the new host profile to the host.

- **A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail**

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: Failed to retrieve appliance storage list

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

- **Enabled SSL protocols configuration parameter is not configured during a host profile remediation process**

Enabled SSL protocols configuration parameter is not configured during a host profile remediation and only the system default protocol tlsv1.2 is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: esxcli system wbem -P <protocol_name>

- **Unable to configure Lockdown Mode settings by using Host Profiles**

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

- **When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts**

Some settings in the VMware config file /etc/vmware/config are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

- **Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error**

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: No valid coredump partition found.

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

- **When a host profile is copied from an ESXi host or a host profile is edited, the user input values are lost**

Some of the host profile keys are generated from hash calculation even when explicit rules for key generation are provided. As a result, when you copy settings from a host or edit a host profile, the user input values in the answer file are lost.

Workaround: In vCenter Server 7.0, when a host profile is copied from an ESXi host or a host profile is modified, the user input settings are preserved.

- **HTTP requests from certain libraries to vSphere might be rejected**

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

POST /sdk HTTP/1.1

SOAPAction

Content-Type: text/xml; charset=utf-8

User-Agent: Java/1.8.0_221

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

- **Editing an advanced options parameter in a host profile and setting a value to false, results in setting the value to true**

When attempting to set a value to false for an advanced option parameter in a host profile, the user interface creates a non-empty string value. Values that are not empty are interpreted as true and the advanced option parameter receives a true value in the host profile.

Workaround: There are two possible workarounds.

- – Set the advanced option parameter to false on a reference ESXi host and copy settings from this host in Host Profiles.
  Note: The host must be compliant with the host profile before modifying the advanced option parameter on the host.
- – Set the advanced option parameter to false on a reference ESXi host and create a host profile from this host. Then copy the host profile settings from the new host profile to the existing host profile.

- **SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process**

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- – To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- – To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

- **You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3**

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command: esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin

- **You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.**

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

VMware vCenter Server Photon OS Security Patches

This document contains the following sections

- Introduction
- Installation Steps
- vCenter Server Appliance Photon OS Security Patches

Introduction

This document tracks the release of 7.0.x patches to the Photon Operating System bundled in VMware vCenter Server.

You can download the deliverables from the Broadcom Support Portal. For download instructions, see Download Broadcom products and software.

Installation Steps

To apply the Photon OS security patches to the vCenter Server Appliance, you can use one of the methods.

- Deploy a new vCenter Server Appliance by using either the GUI or the CLI installer.
  For information about doing a fresh install of the vCenter Server Appliance, see Deploying the vCenter Server Appliance and Platform Services Controller Appliance.
- Upgrade to the version of the vCenter Server Appliance containing the latest Photon OS security patches by using either the GUI or the CLI installer.
  For information about upgrading the vCenter Server Appliance, see Upgrading the vCenter Server Appliance.
- Patch the appliance either by using the appliance shell or the Appliance Management Interface.
  For information on patching the vCenter Server Appliance, see Patching vCenter Server.
- Perform a file-based backup and restore where in the restore process you deploy a new appliance containing the latest Photon OS security patches..
  For information performing a file-based backup and restore of the vCenter Server Appliance, see Restore vCenter Server from a File-Based Backup.
- Migrate a vCenter Server on Windows instance to a version of the vCenter Server Appliance containing the latest Photon OS security patches.
  For information about performing a migration of vCenter Server on Windows to vCenter Server Appliance, see Migrating vCenter Server for Windows to vCenter Server Appliance.

vCenter Server Appliance Photon OS Security Patches

vSphere 7.0 Update 3

vCenter Server 7.0 Update 3v

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
20 May 2025	24730281	vCenter Server 7.0 Update 3v (Security fixes for Photon OS)	xerces-c	3.2.5-1.ph3	CVE-2024-23807 (Score: 9.8)
			httpd	2.4.62-1.ph3	• CVE-2024-27316 (7.5) • CVE-2024-38472 (7.5) • CVE-2024-38475 (9.1) • CVE-2024-39573 (7.5) • CVE-2024-1 (9.1)
			apache-tomcat	8.5.99-1.ph3	CVE-2023-46589 (7.5)
			runc	1.1.4-12.ph3	CVE-2024-21626 (8.6)
			bindutils	9.18.27-1.ph3	• CVE-2023-4408 • CVE-2023-50387 • CVE-2023-50868 • CVE-2023-5517 • CVE-2023-5679 • CVE-2023-6516 • CVE-2024-0760 • CVE-2024-1737 • CVE-2024-1975 • CVE-2024-4076 (All scored 7.5)
			python3-setuptools	57.4.0-2.ph3	CVE-2024-6345 (8.8)
			linux	4.19.325-1.ph3	• CVE-2023-39197 (7.5) • CVE-2023-46838 (7.5) • CVE-2023-52439 (7.8) • CVE-2023-52451 (7.8) • CVE-2023-52340 (7.5) • CVE-2023-6040 (7.8) • CVE-2023-52469 (7.8) • CVE-2024-26883 (7.8) • CVE-2024-26884 (7.8)

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
					• CVE-2024-26898 (7.8) • CVE-2023-52509 (7.8) • CVE-2023-52594 (7.8) • CVE-2023-52599 (7.8) • CVE-2023-52600 (7.8) • CVE-2023-52603 (7.8) • CVE-2023-52604 (7.8) • CVE-2023-52620 (7.6) • CVE-2024-0607 (7.8) • CVE-2024-1086 (7.8) • CVE-2024-23307 (7.8) • CVE-2024-26882 (7.8) • CVE-2024-26934 (7.8) • CVE-2024-27395 (7.8) • CVE-2024-27396 (7.8) • CVE-2024-36971 (7.8) • CVE-2024-39480 (7.8) • CVE-2024-38588 (7.8) • CVE-2024-46738 (7.8) • CVE-2024-46800 (7.8) • CVE-2024-40902 (7.8) • CVE-2024-41087 (7.8) • CVE-2024-42271 (7.8) • CVE-2024-42284 (7.8) • CVE-2024-42285 (7.8) • CVE-2024-42301 (7.8)

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
					• CVE-2024-43858 (7.8) • CVE-2024-44987 (7.8) • CVE-2024-44998 (7.8) • CVE-2024-46673 (7.8) • CVE-2024-46674 (7.8)
			ruby	• 2.5.8-9.ph3	• CVE-2021-33621 (8.8) • CVE-2021-41817 (7.5) • CVE-2021-41819 (7.5) • CVE-2024-49761 (7.5)
			libxml2	2.9.11-13.ph3	• CVE-2024-25062 (7.5) • CVE-2024-34459 (7.5)
			expat	2.2.9-12.ph3	• CVE-2024-45490 (7.5) • CVE-2024-45491 (9.8) • CVE-2024-45492 (9.8)
			libuv	1.34.2-4.ph3	CVE-2024-24806 (9.8)
			python3	3.7.5-34.ph3	CVE-2023-6597 (7.8)
			wget	1.21.3-2.ph3	CVE-2024-38428 (9.1)
			curl	8.1.2-9.ph3	CVE-2024-2398 (7.5)
			krb5	1.17-7.ph3	• CVE-2024-37371 (9.1) • CVE-2024-37370 (7.5)
			sudo	1.9.15p5-1.ph3	CVE-2023-42465 (7)
			nss	3.44-15.ph3	CVE-2024-0743 (7.5)
			less	530-3.ph3	CVE-2024-32487 (9.8)
			dnsmasq	2.90-1.ph3	• CVE-2023-50387 (7.5) • CVE-2023-50868 (7.5)

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
			glibc	2.28-28.ph3	• CVE-2024-33602 • CVE-2024-33600 • CVE-2024-33601 (All 7.6)

vCenter Server 7.0 Update 3d

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
29 March 2022	19480866	vCenter Server 7.0 Update 3d(Security fixes for Photon OS)	c-ares	1.16.1-2.ph3	CVE-2021-3672
			vim	8.2.3408-4.ph3	CVE-2021-3770CVE-2021-3778CVE-2021-3796
			httpd	2.4.51-1.ph3	CVE-2021-33193CVE-2021-34798CVE-2021-36160CVE-2021-40438CVE-2021-39275
			apache-tomcat	8.5.60-4.ph3	CVE-2021-41079
			openssh	7.8p1-10.ph3	CVE-2021-41617
			nettle	3.7.2-2.ph3	CVE-2021-3580
			cpio	2.13-4.ph3	CVE-2021-38185
			util-linux	2.32.1-4.ph3	CVE-2021-37600
			linux	4.19.208-1.ph3	CVE-2020-3702CVE-2021-22543CVE-2021-3653CVE-2021-3656CVE-2021-42008CVE-2021-35039CVE-2021-38160CVE-2021-45485CVE-2021-42252
			ncurses	6.1-3.ph3	CVE-2021-39537
			glibc	2.28-17.ph3	CVE-2021-35942CVE-2021-38604
			atftp	0.7.5-1.ph3	CVE-2021-41054

vCenter Server 7.0 Update 3f

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
12 July 22	20051473	vCenter Server 7.0 Update 3f	apache-tomcat	8.5.72-1.ph3	CVE-2021-42340
			bindutils	9.16.27-1.ph3	CVE-2021-25220
			containerd	1.4.12-1.ph3	CVE-2022-23648
			curl	7.82.0-1.ph3	CVE-2022-22623
				7.82.0-3.ph3	CVE-2022-22576
			cyrus-sasl	2.1.26-17.ph3	CVE-2022-24407
			expat	2.2.9-3.ph3	CVE-2022-22822

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
					CVE-2022-22823
					CVE-2022-22824
					CVE-2022-22825
					CVE-2022-22826
					CVE-2022-22827
				2.2.9-4.ph3	CVE-2021-45960
					CVE-2021-46143
				2.2.9-6.ph3	CVE-2022-23852
					CVE-2022-23990
			glibc	2.28-18.ph3	CVE-2022-23218
					CVE-2022-23219
			httpd	2.4.52-1.ph3	CVE-2021-44790
				2.4.53-1.ph3	CVE-2022-22719
					CVE-2022-22720
					CVE-2022-22721
					CVE-2022-23943
			krb5	1.17-2.ph3	CVE-2020-28196
					CVE-2021-36222
			libxml2	2.9.11-6.ph3	CVE-2022-23308
			linux	4.19.214-3.ph3	CVE-2021-3760
					CVE-2021-41864
				4.19.219-3.ph3	CVE-2020-36385
				4.19.224-1.ph3	CVE-2021-39685
					CVE-2021-39698
					CVE-2021-39713
				4.19.224-2.ph3	CVE-2022-23222
				4.19.225-3.ph3	CVE-2022-0330
				4.19.225-6.ph3	CVE-2022-0435
					CVE-2022-0492
				4.19.229-1.ph3	CVE-2022-1678
				4.19.232-1.ph3	CVE-2022-0847
					CVE-2022-27223
			lua	5.3.5-3.ph3	CVE-2022-28805
			nss	3.44-7.ph3	CVE-2021-43527
			openssl	1.0.2zc-2.ph3	CVE-2022-0778
			pkg-config	0.29.2-3.ph3	CVE-2020-35457
					CVE-2021-27218
			python	3.7.5-17.ph3	CVE-2022-0391
				3.7.5-18.ph3	CVE-2021-3737
			vim	8.2.3408-10.ph3	CVE-2021-4069

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
				8.2.3408-12.ph3	CVE-2021-4136
				8.2.3408-15.ph3	CVE-2021-4187
					CVE-2021-4192
					CVE-2022-0261
					CVE-2022-0318
				8.2.3408-16.ph3	CVE-2022-0128
				8.2.3408-18.ph3	CVE-2021-4173
					CVE-2022-0359
					CVE-2022-0361
					CVE-2022-0408
				8.2.3408-19.ph3	CVE-2022-0392
					CVE-2022-0407
					CVE-2022-0413
					CVE-2022-0443
				8.2.3408-20.ph3	CVE-2022-0368
				8.2.3408-22.ph3	CVE-2022-0554
					CVE-2022-0629
					CVE-2022-0685
					CVE-2022-0729
				8.2.3408-23.ph3	CVE-2022-0572
				8.2.3408-25.ph3	CVE-2022-0417
				8.2.3408-5.ph3	CVE-2021-3872
				8.2.3408-7.ph3	CVE-2021-3973
					CVE-2021-3974
				8.2.3408-8.ph3	CVE-2021-3903
					CVE-2021-3927
					CVE-2021-3928
				8.2.3408-9.ph3	CVE-2021-3984
					CVE-2021-4019
				8.2.4646-1.ph3	CVE-2022-0943
					CVE-2022-1154
				8.2.4647-1.ph3	CVE-2022-1160
				8.2.4827-1.ph3	CVE-2022-1381
				8.2.4925-1.ph3	CVE-2022-1616
					CVE-2022-1619
					CVE-2022-1620
					CVE-2022-1621
					CVE-2022-1629
			zlib	1.2.11-2.ph3	CVE-2018-25032

vCenter Server 7.0 Update 3i

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
08 December 2022	20845200	vCenter Server 7.0 Update 3i(Security fixes for Photon OS)	bindutils	9.16.33-1.ph3	CVE-2022-2795
					CVE-2022-3080
					CVE-2022-38177
					CVE-2022-38178
			cifs-utils	6.8-4.ph3	CVE-2022-27239
			curl	curl-7.83.1-3.ph3	CVE-2022-27775
					CVE-2022-27780
					CVE-2022-27781
					CVE-2022-27782
			expat	2.2.9-10.ph3	CVE-2022-40674
				2.2.9-8.ph3	CVE-2022-25314
					CVE-2022-25315
			glib	2.58.0-9.ph3	CVE-2021-3800
			glibc	2.28-22.ph3	CVE-2021-3999
			gnutls	3.6.16-3.ph3	CVE-2022-2509
			httpd	2.4.54-1.ph3	CVE-2022-26377
					CVE-2022-28615
					CVE-2022-29404
					CVE-2022-30522
					CVE-2022-30556
					CVE-2022-31813
			libarchive	3.3.3-8.ph3	CVE-2021-23177
					CVE-2021-31566
			libtirpc	1.1.4-2.ph3	CVE-2021-46828
			libxml2	2.9.11-8.ph3	CVE-2022-2309
			libxslt	1.1.34-1.ph3	CVE-2021-30560
			linux	4.19.241-1.ph3	CVE-2022-1055
					CVE-2022-28356
				4.19.245-1.ph3	CVE-2022-29581
				4.19.247-2.ph3	CVE-2022-1966
					CVE-2022-32250
					CVE-2022-32981
				4.19.256-1.ph3	CVE-2021-33656
					CVE-2022-36946
			lua	5.3.5-4.ph3	CVE-2022-33099
			lz4	1.9.2-1.ph3	CVE-2019-17543
				1.9.3-2.ph3	CVE-2021-3520
			openldap	2.4.57-3.ph3	CVE-2022-29155

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
			openssl	openssl-1.0.2ze-3.ph3	CVE-2022-1292
					CVE-2022-2068
			postgresql	10.22-1.ph3	CVE-2022-2625
			python	3.7.5-21.ph3	CVE-2015-20107
			runc	1.1.3-3.ph3	CVE-2022-29162
			systemd	239-44.ph3	CVE-2022-2526
			vim	vim-8.2.5169-1.ph3	CVE-2022-1733
					CVE-2022-1735
					CVE-2022-1769
					CVE-2022-1785
					CVE-2022-1796
					CVE-2022-1851
					CVE-2022-1886
					CVE-2022-1898
					CVE-2022-1927
					CVE-2022-1942
					CVE-2022-2124
					CVE-2022-2125
					CVE-2022-2126
					CVE-2022-2129
					CVE-2022-2175
					CVE-2022-2182
					CVE-2022-2183
					CVE-2022-2206
					CVE-2022-2207
					CVE-2022-2210
			zlib	1.2.11-3.ph3	CVE-2022-37434

vCenter Server 7.0 Update 3l

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
30 March 2023	21477706	vCenter Server 7.0 Update 3l(Security fixes for Photon OS)	apache-ant	1.10.12-1.ph3	CVE-2017-1000487 CVE-2022-24839
			binutils	2.32-7.ph3	CVE-2021-45078 CVE-2021-37322 CVE-2018-1000876
			curl	7.86.0-3.ph3	CVE-2022-32207 CVE-2022-22576 CVE-2022-27782 CVE-2022-27781 CVE-2022-27775

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
					CVE-2021-22946 CVE-2021-22926 CVE-2020-8286 CVE-2020-8285
			grub2	2.06-4.ph3	CVE-2022-2601
			linux	4.19.269-3.ph3	CVE-2022-3649 CVE-2022-3643 CVE-2022-42896 CVE-2022-20568 CVE-2022-2327
			pcre	8.44-2.ph3	CVE-2019-20838
			ruby	2.5.8-4.ph3	CVE-2020-25613 CVE-2020-10663
			samba-client	4.14.14-1.ph3	CVE-2021-23192 CVE-2022-2031 CVE-2022-32744 CVE-2022-32745

vCenter Server 7.0 Update 3o

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
28 September 2023	22357613	vCenter Server 7.0 Update 3o(Security fixes for Photon OS)	gnutls	3.6.16-4.ph3	CVE-2023-0361
			vim	8.2.5169-5.ph3	CVE-2022-47024
					CVE-2023-0049
					CVE-2023-0051
					CVE-2023-0054
					CVE-2023-0433
			httpd	2.4.56-1.ph3	CVE-2006-20001
					CVE-2022-36760
					CVE-2023-25690
					CVE-2023-27522
			apache-tomcat	8.5.84-2.ph3	CVE-2022-42252
					CVE-2022-45143
			libtasn1	4.14-2.ph3	CVE-2021-46848
			krb5	1.17-4.ph3	CVE-2022-42898
			tar	1.30-6.ph3	CVE-2022-48303
			sudo	1.9.5-5.ph3	CVE-2023-22809
			nss	3.44-9.ph3	CVE-2019-17006
					CVE-2020-25648
			bindutils	9.16.38-1.ph3	CVE-2022-3736
			openssl	1.0.2zg-1.ph3	CVE-2022-4450
					CVE-2023-0215

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
			libarchive	3.3.3-9.ph3	CVE-2022-36227
			sysstat	12.7.1-1.ph3	CVE-2022-39377
			linux	4.19.277-4.ph3	CVE-2023-1281
					CVE-2023-26545
					CVE-2023-23559
			containerd	1.6.8-3.ph3	CVE-2023-25173
			libxml2	2.9.11-9.ph3	CVE-2022-40303
					CVE-2022-40304
			expat	2.2.9-11.ph3	CVE-2020-10735
			python3	3.7.5-26.ph3	CVE-2020-10735
					CVE-2022-37454
					CVE-2022-45061
			dnsmasq	2.85-3.ph3	CVE-2022-0934
			pkg-config	0.29.2-4.ph3	CVE-2021-3800
			curl	7.86.0-5.ph3	CVE-2023-23914
					CVE-2023-23916
					CVE-2023-27535
					CVE-2023-27536
			e2fsprogs	1.46.5-2.ph3	CVE-2022-1304

vCenter Server 7.0 Update 3q

Release Date	Build Number	Patch Name	Affect Package	New Package Version	CVEs Addressed
21 May 2024	23788036	vCenter Server 7.0 Update 3q(Security fixes for Photon OS)	apache-tomcat	8.5.88-2.ph3	CVE-2023-28709
			apr-util	1.6.1-5.ph3	CVE-2022-25147
			bindutils	9.16.42-3.ph3	CVE-2023-3341CVE-2023-2829CVE-2023-2828 CVE-2023-2911
			c-ares	1.19.1-1.ph3	CVE-2023-32067
			cloud-init	22.4.2-5.ph3	CVE-2023-1786
			curl	8.1.2-4.ph3	CVE-2023-38039CVE-2023-38545 CVE-2023-38456
			dmidecode	3.5-1.ph3	CVE-2023-30630
			dnsmasq	2.85-4.ph3	CVE-2023-28450
			elfutils	0.176-3.ph3	CVE-2021-33294CVE-2020-21047
			freetype2	2.9.1-5.ph3	CVE-2023-2004
			gawk	4.2.1-2.ph3	CVE-2023-4156

gdb	10.1-5.ph3	CVE-2018-25032CVE-2021-3549 CVE-2022-38533 CVE-2022-4285CVE-2023-1972 CVE-2023-25584 CVE-2023-25585 CVE-2023-25588
glibc	2.28-24.ph3	CVE-2023-4813
grub2	2.06-9.ph3	CVE-2023-4692 CVE-2023-4693CVE-2022-28736CVE-2021-3697
httpd	2.4.58-1.ph3	CVE-2023-31122
krb5	1.17-5.ph3	CVE-2023-36054
libldb	2.6.2-1.ph3	CVE-2023-0614
libssh2	1.9.0-3.ph3	CVE-2020-22218
libuv	1.34.2-3.ph3	CVE-2020-8252
libxml2	2.9.11-11.ph3	CVE-2023-29469 CVE-2023-28484CVE-2023-45322
linux	4.19.297-1.ph3	CVE-2023-1611CVE-2023-1076 CVE-2023-1077CVE-2021-3759CVE-2023-2124CVE-2023-4128CVE-2023-2007CVE-2023-42753CVE-2023-42754
nss	3.44-11.ph3	CVE-2022-36320 CVE-2019-11729CVE-2019-11745
ntp	4.2.8p16-1.ph3	CVE-2023-26551 CVE-2023-26555
open-vm-tools	12.2.0-5.ph3	CVE-2023-20867CVE-2023-20900CVE-2023-34058 CVE-2023-34059
openldap	2.4.57-4.ph3	CVE-2023-2953
openssh	7.8p1-17.ph3	CVE-2023-38408CVE-2023-51385
perl	5.28.0-8.ph3	CVE-2023-31486
postgresql13	13.13-1.ph3	CVE-2023-2454 CVE-2023-2455
procps-ng	3.3.15-4.ph3	CVE-2023-4016
python3	3.7.5-32.ph3	CVE-2023-24329CVE-2022-48565 CVE-2022-48566 CVE-2022-48560

					CVE-2022-48564CVE-2007-4559CVE-2023-40217
			runc	1.1.4-9.ph3	CVE-2023-27561CVE-2023-25809
			samba-client	4.17.12-1.ph3	CVE-2023-3961
			shadow	4.6-7.ph3	CVE-2023-29383
			sqlite	3.35.5-2.ph3	CVE-2021-31239
			systemd	239-51.ph3	CVE-2023-26604CVE-2023-26604
			tcpdump	4.99.4-1.ph3	CVE-2020-8036
			traceroute	2.1.3-1.ph3	CVE-2023-46316
			unzip	6.0-18.ph3	CVE-2022-0529 CVE-2022-0530
			vim	8.2.5169-14.ph3	CVE-2023-1264 CVE-2023-1175 CVE-2023-1170 CVE-2022-3352CVE-2022-3256 CVE-2022-3235 CVE-2022-4141 CVE-2022-3099CVE-2022-2874 CVE-2022-2343 CVE-2022-3134 CVE-2022-2849CVE-2022-2285 CVE-2022-3234 CVE-2022-3297 CVE-2022-2286CVE-2022-2345 CVE-2022-2581 CVE-2022-2522 CVE-2022-2889 CVE-2022-3296 CVE-2022-2598 CVE-2022-2982 CVE-2022-2845CVE-2022-2571 CVE-2022-3016 CVE-2022-2289 CVE-2022-2344CVE-2022-3037 CVE-2022-2287 CVE-2022-2257 CVE-2022-2284CVE-2022-2264, CVE-2022-2980 CVE-2022-2817 CVE-2022-2580 CVE-2022-2288 CVE-2022-2816

					CVE-2022-2862 CVE-2022-2923CVE-2022-2304 CVE-2022-3491 CVE-2022-4293 CVE-2022-3705CVE-2022-3153 CVE-2022-3278CVE-2023-2426CVE-2023-2610CVE-2023-2609CVE-2023-5344 CVE-2023-5441 CVE-2023-5535CVE-2023-46246
			xerces-c	3.2.4-1.ph3	CVE-2012-0880
			xinetd	2.3.15-10.ph3	CVE-2013-4342
			zlib	1.2.11-5.ph3	CVE-2023-45853
			python3-certifi	2023.11.17-1	CVE-2023-37920

vSphere 7.0 Update 2

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
24 August 2021	18356314	vCenter Server 7.0 Update 2c(Security fixes for Photon OS)	apache-tomcat	8.5.60-2.ph3	CVE-2021-25122
					CVE-2021-25329
			atftp	0.7.2-2.ph3	CVE-2020-6097
			bindutils	9.16.6-2.ph3	CVE-2020-8625
			c-ares	1.16.1-1.ph3	CVE-2020-8277
			containerd	1.4.4-1.ph3	CVE-2021-21334
			dnsmasq	2.82-2.ph3	CVE-2020-25681
					CVE-2020-25682
			glib	2.58.0-7.ph3	CVE-2021-27218
					CVE-2021-27219
			glibc	2.28-12.ph3	CVE-2021-3326
			gnutls	3.6.15-3.ph3	CVE-2021-20231
			grub2	2.06~rc1-1.ph3	CVE-2021-20232
					CVE-2020-14372
					CVE-2020-25632
					CVE-2020-25647
					CVE-2020-27749
					CVE-2020-27779
					CVE-2021-20225
					CVE-2021-20233
					CVE-2021-3418
			linux	4.19.186-3.ph3	CVE-2020-29569
					CVE-2020-29661

Release Date	Build Number	Patch Name	Affected Package	New Package Versions	CVEs Addressed
					CVE-2021-3347
					CVE-2021-26930
					CVE-2021-27365
					CVE-2021-28660
					CVE-2021-28972
			nettle	3.7.2-1.ph3	CVE-2021-20305
			nss	3.44-6.ph3	CVE-2020-12403
			openldap	2.4.57-2.ph3	CVE-2020-36221
					CVE-2020-36222
					CVE-2020-36223
					CVE-2020-36224
					CVE-2020-36225
					CVE-2020-36226
					CVE-2020-36227
					CVE-2020-36228
					CVE-2020-36229
					CVE-2020-36230
					CVE-2021-27212
			openssl	1.0.2y-1.ph3	CVE-2021-23839
					CVE-2021-23840
			runc	1.0.0.rc93-2.ph3	CVE-2021-30465
			sudo	1.9.5-3.ph3	CVE-2021-23240
					CVE-2021-3156

ESXi Update and Patch Release Notes

VMware ESXi 7.0 Update 3w Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Upgrade Notes
- Patch Download and Installation
- Resolved Issues
- Known Issues from Previous Releases

Introduction

VMware ESXi 7.0 Update 3w | 15 JUL 2025 | Build 24784741
Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3w, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3w. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- This release resolves CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, and CVE-2025-41239. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0013.
- This release resolves CVE-2025-2884. Broadcom has evaluated the severity of this issue to be in the moderate severity range.

Patches Contained in This Release

This release of ESXi 7.0 Update 3w delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3w-24784741-depot.zip
Build:	24784741
Download Size:	419.5 MB
md5sum:	bc919e2febfb81b767e85e4fd33e75b8
sha256checksum:	11e8c973918df2f0a9720995f8481deaa8d6b56daf4e931971a0b903a871b944
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.150.24784741	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.150.24784741	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3w-24784741	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3w-24784741-standard
ESXi-7.0U3w-24784741-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi 7.0 U3w - 24784741	JULY 15 2025	Security	Security only

Upgrade Notes

The supported upgrade path from ESXi 7.0 Update 3w to ESXi 8.x is ESXi 8.0 Update 3g.

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

See these KBs for details on the authenticated online and offline download: 390121, 390098, and 389276.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.150.24784741

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_native-misc-drivers_7.0.3-0.150.24784741

	• VMware_bootbank_vsan_7.0.3-0.150.24784741 • VMware_bootbank_bmcal_7.0.3-0.150.24784741 • VMware_bootbank_esx-xserver_7.0.3-0.150.24784741 • VMware_bootbank_gc_7.0.3-0.150.24784741 • VMware_bootbank_esx-base_7.0.3-0.150.24784741 • VMware_bootbank_esxio-combiner_7.0.3-0.150.24784741 • VMware_bootbank_trx_7.0.3-0.150.24784741 • VMware_bootbank_cpu-microcode_7.0.3-0.150.24784741 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.150.24784741 • VMware_bootbank_vsanhealth_7.0.3-0.150.24784741 • VMware_bootbank_crx_7.0.3-0.150.24784741 • VMware_bootbank_vdfs_7.0.3-0.150.24784741
PRs Fixed	N/A
CVE numbers	CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239, CVE-2025-2884

The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

This patch updates the `esx-base` VIB. Due to their dependency with the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `native-misc-drivers`, `vsan`, `bmcal`, `esx-xserver`, `gc`, `esx-base`, `esxio-combiner`, `trx`, `cpu-microcode`, `esx-dvfilter-generic-fastpath`, `vsanhealth`, `crx`, and `vdfs` .

This patch resolves the following issues:

- This release resolves CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, and CVE-2025-41239. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0013.
- This release resolves CVE-2025-2884. Broadcom has evaluated the severity of this issue to be in the moderate severity range.

esx-update_7.0.3-0.150.24784741

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.150.24784741 • VMware_bootbank_esx-update_7.0.3-0.150.24784741
PRs Fixed	N/A
CVE numbers	N/A

Due to their dependency on the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `loadesx` and `esx-update` .

ESXi-7.0U3w-24784741-standard

Profile Name	ESXi-7.0U3w-24784741-standard
Build	For build information, see the Patches Contained in This Release section.
Vendor	Broadcom, Inc.
Release Date	July 15, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_native-misc-drivers_7.0.3-0.150.24784741 • VMware_bootbank_vsan_7.0.3-0.150.24784741 • VMware_bootbank_bmcal_7.0.3-0.150.24784741 • VMware_bootbank_esx-xserver_7.0.3-0.150.24784741 • VMware_bootbank_gc_7.0.3-0.150.24784741 • VMware_bootbank_esx-base_7.0.3-0.150.24784741 • VMware_bootbank_esxio-combiner_7.0.3-0.150.24784741 • VMware_bootbank_trx_7.0.3-0.150.24784741 • VMware_bootbank_cpu-microcode_7.0.3-0.150.24784741 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.150.24784741 • VMware_bootbank_vsanhealth_7.0.3-0.150.24784741 • VMware_bootbank_crx_7.0.3-0.150.24784741 • VMware_bootbank_vdfs_7.0.3-0.150.24784741 • VMware_bootbank_esx-update_7.0.3-0.150.24784741 • VMware_bootbank_loadesx_7.0.3-0.150.24784741
PRs Fixed	N/A
Related CVE numbers	CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239, CVE-2025-2884

This patch updates the following issues:

- This release resolves CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, and CVE-2025-41239. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0013.
- This release resolves CVE-2025-2884. Broadcom has evaluated the severity of this issue to be in the moderate severity range.

ESXi-7.0U3w-24784741-no-tools

Profile Name	ESXi-7.0U3w-24784741-no-tools
Build	For build information, see the Patches Contained in This Release section.
Vendor	Broadcom, Inc.
Release Date	July 15, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_native-misc-drivers_7.0.3-0.150.24784741

	• VMware_bootbank_vsan_7.0.3-0.150.24784741 • VMware_bootbank_bmcal_7.0.3-0.150.24784741 • VMware_bootbank_esx-xserver_7.0.3-0.150.24784741 • VMware_bootbank_gc_7.0.3-0.150.24784741 • VMware_bootbank_esx-base_7.0.3-0.150.24784741 • VMware_bootbank_esxio-combiner_7.0.3-0.150.24784741 • VMware_bootbank_trx_7.0.3-0.150.24784741 • VMware_bootbank_cpu-microcode_7.0.3-0.150.24784741 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.150.24784741 • VMware_bootbank_vsanhealth_7.0.3-0.150.24784741 • VMware_bootbank_crx_7.0.3-0.150.24784741 • VMware_bootbank_vdfs_7.0.3-0.150.24784741 • VMware_bootbank_esx-update_7.0.3-0.150.24784741 • VMware_bootbank_loadesx_7.0.3-0.150.24784741
PRs Fixed	N/A
Related CVE numbers	CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239, CVE-2025-2884

This patch updates the following issues:

- This release resolves CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, and CVE-2025-41239. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0013.
- This release resolves CVE-2025-2884. Broadcom has evaluated the severity of this issue to be in the moderate severity range.

ESXi 7.0 U3w - 24784741

Name	ESXi
Version	ESXi 7.0 U3w - 24784741
Release Date	July 15, 2025
Category	Security
Affected Components	• ESXi Component - core ESXi • ESXi Install/Upgrade
PRs Fixed	N/A
Related CVE numbers	CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239, CVE-2025-2884

This patch resolves the issues listed in the ESXi-7.0U3w-24784741-standard image profile.

Known Issues from Previous Releases

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Corrupted VFAT partitions from a vSphere 6.7 environment might cause upgrades to ESXi 7.x to fail

Due to corrupted VFAT partitions from a vSphere 6.7 environment, repartitioning the boot disks of an ESXi host might fail during an upgrade to ESXi 7.x. As a result, you might see the following errors:

When upgrading to ESXi 7.0 Update 3l, the operation fails with a purple diagnostic screen and/or an error such as:

- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to calculate size for temporary Ramdisk: <error>.`
- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to copy files to Ramdisk: <error>.`
  If you use an ISO installer, you see the errors, but no purple diagnostic screen.

When upgrading to an ESXi 7.x version earlier than 7.0 Update 3l, you might see:

- Logs such as `ramdisk (root) is full` in the `vmkwarning.log` file.
- Unexpected rollback to ESXi 6.5 or 6.7 on reboot.
- The `/bootbank` ,`/altbootbank` , and ESX-OSData partitions are not present.

Workaround: You must first remediate the corrupted partitions before completing the upgrade to ESXi 7.x. For more details, see VMware knowledge base article 91136.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the requirement cannot be satisfied within the ImageProfile. Please refer to the log file for more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
 The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
 Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s)`.

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU`.

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer.`

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq “slpd”} | Set-VMHostService -policy “off”$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq “slpd”} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx` , the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1`.

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set --tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer": { "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"`, run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo`"

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo`"

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first

disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command:
   `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command:
   `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command:
   `esxcli network firewall load.`
5. Start the hostd service by using the command:
   `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats`, you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835`.

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0`.

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set -o /USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.

2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

vSAN Issues

PR 2962316: vSAN File Service does not support NFSv4 delegations

vSAN File Service does not support NFSv4 delegations in this release.

Workaround: None

When rebooting a vSAN host, other hosts in the vSAN cluster enter a partitioned state

During ESXi shutdown, hosts in a vSAN cluster can enter a state where they can transmit but not receive data. Depending of the exact timing and duration of this state, this state can lead to unexpected role changes in the vSAN distributed cluster membership, monitoring, and directory service (CMMDS). Consequently, vSAN hosts might continually attempt to reform a cluster with the rebooting host or send CMMDS updates through the rebooting host, which is unresponsive to incoming traffic. As a result, in the vSAN Health monitoring you see `vSAN Cluster Partition` alarms.

Workaround: Before rebooting a vSAN host, identify all vmknics on the host with tags `VSAN` , `VSANWitness` , or `VSANExternal` , take note of which vSAN tag is used on each vmknic, and remove the tags. After rebooting, reapply the tags for vSAN traffic by type and vmknic.

PR 3235496: Applications on a vSAN cluster become intermittently unresponsive

If the advanced option `preferHT` is enabled on an AMD server in a vSAN cluster, the virtual CPUs of a virtual machine run on the same last level cache. When the virtual CPUs are all very busy and an NVMe thread to handle I/Os happens to run also on the same last level cache, the NVMe thread takes very long to complete, because it competes for CPU resources with the busy VMs. As a result, the I/O latency is very high and might lead to intermittent unresponsiveness of storage and applications on the vSAN cluster. In the backlog, you see errors such as `Lost access to volume <uuid> due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.`

Workaround: Use the command `esxcli system settings advanced set -o /Misc/vmknvmeCwYield -I 0` to avoid competition between the NVMe completion queue and busy virtual CPUs.

VMware ESXi 7.0 Update 3v Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues
- Known Issues from Previous Releases

Introduction

VMware ESXi 7.0 Update 3v | 20 MAY 2025 | Build 24723872 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3v, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3v. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

This release resolves CVE-2025-41226, CVE-2025-41227, and CVE-2025-41228. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0010.

ESXi 7.0 Update 3v adds support for vSphere Quick Boot to the following:

Drivers:

- AMD
  - AMD Instinct MI Series Driver
- Intel
  - Intel vRAN Baseband Driver
  - Intel Platform Monitoring Technology Driver
  - Intel Data Center Graphics Driver

Servers

- CISCO
  - UCSC-C240-M7SX
  - UCSC-C245-M8SX
- HPE
  - HPE Alletra Storage Server 4120
  - HPE ProLiant DL145 Gen11
- Supermicro
  - AS-2025HS-TNR

Patches Contained in This Release

This release of ESXi 7.0 Update 3v delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3v-24723872-depot.zip
Build:	24723872
Download Size:	585 MB
md5sum:	31d75becb9fff8f9588b9d7b867a28c4
sha256checksum:	b9402fd4152cfd79a5e019c5445e83991f96d67b9718290a0aa45f224a3ab997
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.145.24723872	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.145.24723872	Bugfix	Critical
Broadcom NetXtreme I ESX VMKAPI ethernet driver	Broadcom-ntg3_4.1.15.0-4vmw.703.0.145.24723872	Bugfix	Critical
VMware NVMe over TCP Driver	VMware-NVMeoF-TCP_1.0.0.7-1vmw.703.0.145.24723872	Bugfix	Critical

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.140.24723868	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.140.24723868	Security	Critical
ESXi Tools Component	VMware-VM-Tools_12.5.1.24649672-24723868	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3v-24723872	Bugfix	Critical	Security and Bugfix
ESXi70U3sv-24723868	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3v-24723872-standard
ESXi-7.0U3v-24723872-no-tools
ESXi-7.0U3sv-24723868-standard
ESXi-7.0U3sv-24723868-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi 7.0 U3v - 24723872	MAY 20 2025	Bugfix	Security and Bugfix
ESXi 7.0 U3sv - 24723868	MAY 20 2025	Security	Security only

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

See these KBs for details on the authenticated online and offline download: 390121, 390098, and 389276.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.145.24723872

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_native-misc-drivers_7.0.3-0.145.24723872 • VMware_bootbank_vsan_7.0.3-0.145.24723872 • VMware_bootbank_bmcal_7.0.3-0.145.24723872 • VMware_bootbank_esx-xserver_7.0.3-0.145.24723872 • VMware_bootbank_gc_7.0.3-0.145.24723872 • VMware_bootbank_esx-base_7.0.3-0.145.24723872 • VMware_bootbank_esxio-combiner_7.0.3-0.145.24723872 • VMware_bootbank_trx_7.0.3-0.145.24723872 • VMware_bootbank_cpu-microcode_7.0.3-0.145.24723872 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.145.24723872 • VMware_bootbank_vsanhealth_7.0.3-0.145.24723872 • VMware_bootbank_crx_7.0.3-0.145.24723872 • VMware_bootbank_vdfs_7.0.3-0.145.24723872
PRs Fixed	3406035, 3477734, 3489859, 3352051, 3457552, 3485174, 3469639, 3470731, 3485586, 3484794, 3484793, 3484786, 3477773, 3469106, 3477257, 3476746, 3475049, 3454755, 3469189, 3466996, 3458045, 3435833, 3447991, 3443815, 3432572, 3432690, 3441101, 3404668, 3434172, 3437311, 3371201, 3367834, 3398462, 3410295, 3390998, 3398458, 3388843, 3398467, 3430801, 3408807, 3420117, 3417327, 3423849, 3417227, 3417328, 3404126, 3408129, 3408008, 3408126, 3398534, 3400360, 3406033, 3398361, 3398279, 3407212, 3411695, 3396010, 3412537, 3352007, 3404202, 3402976, 3396464, 3407529, 3408143, 3336865, 3403867, 3389767, 3366075, 3365863, 3404507, 3403906, 3405760, 3401554, 3398537, 3355390, 3359530, 3393549, 3367426, 3359386, 3382561, 3358960

CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

This patch updates the `native-misc-drivers, vsan, bmcal, esx-xserver, gc, esx-base, esxio-combiner, trx, cpu-microcode, esx-dvfilter-generic-fastpath, vsanhealth, crx` , and `vdfs` VIBs to resolve the following issues:

PR 3406033: ESXi host fails with a purple diagnostic screen due to a rare physical CPU (PCPU) lockup

In the vSphere Client, when you use the **Delete from Disk** option to remove a virtual machine from a vCenter system and delete all VM files from the datastore, including the configuration file and virtual disk files, if any of the files is corrupted, a rare issue with handling corrupted files in the delete path might lead to a PCPU lockup. As a result, the ESXi host fails with a purple diagnostic screen and a message such as `NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release.

PR 3484786: ESXi installation on an iSCSI LUN fails as the ESXi iSCSI Boot Firmware Table (iBFT) module fails to discover the LUN

In some cases, the iBFT control structure might have an optional expansion for which the ESXi vmkibft module doesn't have a proper check. As a result, iSCSI LUN discovery by using iBFT might fail and cause failure of the ESXi installation on the iSCSI LUN.

This issue is resolved in this release.

PR 3423217: You see vendor name of some Solidigm NVMe devices as Unknown

In the ESXi Host Client, under **Manage > Hardware > PCI Devices**, and in the vSphere Client, under **Host > Configure > Hardware > PCI Devices > All PCI Devices**, you might see the vendor name of some Solidigm NVMe devices as `Unknown.`

This issue is resolved in this release.

PR 3398537: ESXi host fails with a purple diagnostic screen due to an I/O race with an error PSOD @BlueScreen: ASSERT bora/lib/misc/bitvector.c:632

Due to a rare I/O race condition on virtual machines backed by a vSphere Virtual Volume, the ESXi host might fail with a purple diagnostic screen and an error such as `PSOD @BlueScreen: ASSERT bora/lib/misc/bitvector.c:632.`

This issue is resolved in this release.

PR 3371201: The hostd service might generate core dumps during upgrade from ESXi 6.7 to 7.x when SNMP traps are configured

In very rare cases, a missing SNMP port value when SNMP traps are configured during an upgrade from ESXi 6.7 to 7.x, might lead to hostd core dumps.

This issue is resolved in this release.

PR 3352051: Syslog configuration changes in a host profile that you use to provision ESXi host with Auto Deploy stateful install do not persist across reboots

If you change the syslog configuration of a host profile and provision ESXi hosts with that profile by using the Auto Deploy stateful install, changes might not persist after the hosts reboot.

This issue is resolved in this release.

PR 3396010: Controller VMs with direct I/O devices in third-party hyper converged infrastructure environments experience guest kernel soft lockups

A rare race condition between the interrupt virtualization and the VMkernel CPU scheduler in an ESXi host might result in guest kernel soft lockups on controller VMs with direct I/O devices in third-party hyper converged infrastructure environments. The soft locks cause virtual machines in the entire cluster to lose NFS storage connectivity and I/O access.

This issue is resolved in this release.

PR 3359386: If the Latency Sensitivity parameter of a virtual machine is set to High, you cannot add memory to that VM when powered off

If you use the vSphere Client to set the `Latency Sensitivity` parameter of a VM to `High` , attempts to add memory to such a VM when powered off might fail with an error such as `A specified parameter was not correct: spec.memoryAllocation` .

This issue is resolved in this release.

PR 3403867: Setting the CPU limit to 0 makes virtual machines unresponsive

If for any reason you set the CPU limit of running virtual machines to `0` , this causes CPU starvation and the VMs become unresponsive.

This issue is resolved in this release.

PR 3457552: You might see multiple hardware sensor alerts due to a Baseboard Management Controller (BMC) issue

An underlying BMC issue might cause ESXi hardware health monitoring to produce multiple alerts for hardware sensors on ESXi hosts, which you see in the vSphere Client under **Monitor > Tasks and Events**.

This issue is resolved in this release. The fix logs raw sensor data directly from IPMI to provide a data point to debug possible BMC issues that cause false alerts but cannot prevent BMC issues from occuring.

PR 3484794: Restoring the iSCSI configurations on an ESXi host might fail during boot due to stale entries in the ConfigStore database

If the ConfigStore database on an ESXi host has stale iSCSI configurations related to hardware iSCSI adapters, the iSCSI jumpstart might fail and restoring the iSCSI configuration on that host also fails during boot.

This issue is resolved in this release.

PR 3484793: Discovery of iSCSI dynamic targets, LUNs, and datastores fails on ESXi host reboot

In some cases, dynamic discovery of targets in systems that use dynamic discovery addresses for iSCSI configuration might fail. As a result, you do not see iSCSI targets, LUNs, and datastores after a reboot of ESXi hosts. The dynamic discovery of iSCSI targets might also fail when the Challenge-Handshake Authentication Protocol (CHAP) is active on the ESXi host.

This issue is resolved in this release.

PR 3425364: Setting `cloud-init guestInfo` variables by regular users in the guest results into an error

Starting with ESXi 7.0 Update 3v, setting `cloud-init guestInfo` variables by regular users in the guest results into an error due to design changes.

This issue is resolved in this release. For more information, see KB 377267.

PR 3458283: A rare Baseboard Management Controller (BMC) issue might cause some applications to become unresponsive

If an application sends an IPMI request to the BMC while it resets, such requests remain indefinitely pending and cause the applications to become unresponsive.

This issue is resolved in this release. The fix updates the IPMI driver to handle such conditions.

PR 3485174: Guest OS might mark file system read-only after repeated I/O failure which can cause Kubernetes control plane nodes to go into Read-only mode

An issue with the check for max allowed memory address in memory mapping code during I/O processing at virtual SCSI might cause a guest OS on an ESXi host to mark guest file system as read-only. As a result, Kubernetes control plane nodes might go into Read-only mode. In the vmkernel logs, you see multiple error messages such as `failed to pin: I/O error.`

This issue is resolved in this release.

PR 3470731: Unsupported SCSI Read Mode Sense Page commands to a Raw Disk Mapping (RDM) target might cause virtual machines to become unresponsive

A large number of unsupported SCSI Read Mode Sense Page commands to a RDM target from a VM configured with an RDM device might exceed the storage heap and cause both the datastore and the VM to become unresponsive.

This issue is resolved in this release. The fix prevents blocking VM I/O operations by optimizing the handling of unsupported SCSI commands or mode pages. Specifically, in passthrough mode used for RDM devices, the system no longer attempts to process such unsupported commands in a way that consumes storage heap resources.

PR 3398467: vSphere Virtual Volumes daemon fails after converting a VASA provider from external to internal

Due to an issue with handling IDs during an unbind operation for some vSphere API for Storage Awareness (VASA) providers, in some tasks such as converting a VASA provider from external to internal, the vSphere Virtual Volumes daemon vvold might fail as it cannot map unique IDs.

This issue is resolved in this release. With the fix, vvold gracefully handles such conditions and stops the unbind operation with message in the logs instead of failing.

PR 3388843: You cannot activate Kernel DMA Protection on a virtual machine with Windows OS and Intel processor

When virtual Input-Output Memory Management Unit (vIOMMU) is active on a virtual machine with Windows OS and an Intel CPU, you might not be able to activate Kernel DMA Protection.

This issue is resolved in this release. The fix adds `acpi.dmar.enableDMAProtection=TRUE` to the vmx advanced settings that you can use if required.

PR 3469106: ESXi hosts intermittently disconnect from the Active Directory domain or from vCenter

Memory leaks might occur in Likewise during Active Directory operations or if smart card authentication is active on an ESXi host. As a result, Likewise processes might run out of memory and ESXi hosts intermittently disconnect from the Active Directory domain or from vCenter. In the `/var/log/vmkernel.log` file, you see messages similar to:

```
yyyy-mm-dd In(182) vmkernel: cpu72:2110465)uw.2110464 (44739) requires 1024 KB, asked 1024 KB from likewise (792) which has 93112 KB occupied and 72 KB available.
```

```
yyyy-mm-dd In(182) vmkernel: cpu72:2110465)Admission failure in path: host/vim/vmvisor/likewise:lwsmd.2110464:uw.2110464
```

In the `hostd-probe.log` file you see a message such as: `hostd detected to be non-responsive.`

This issue is resolved in this release. The fix adds a system service that monitors Likewise memory usage and restarts relevant services in case memory consumption approaches Likewise limits.

PR 3477734: ESXi host fails with a purple diagnostic screen while activating HClock

If for some reason an ESXi host fails to allocate memory for the activation of the HClock capability, the error handling goes into CPU wait state while it still holds a lock. As a result, the host fails with a purple diagnostic screen, and you see backtraces such as:

```
[0x2b8c]RCU_WaitForGracePeriod@vmkernel#nover stack:
[0xa000]vmk_HashRelease@vmkernel#nover+ stack:
```

```
[0xa0000]NetSchedHClkConnect@(netsched_hclk)#<None> stack:
```

This issue is resolved in this release.

PR 3489859: Migration of virtual machines fails with an error "Failed to allocate migration heap" on the source ESXi host

In very rare cases, if a virtual machine powers off before a running migration completes, ESXi might fail to clean up the migration heap. If the memory leak continues over time, the migration heap might be exhausted, and virtual machines cannot migrate from such ESXi hosts.

This issue is resolved in this release.

PR 3499302: If a virtual machine migrates to an ESXi host undergoing NSX update, the Distributed Firewall rule might be detached from that host

During NSX update or upgrade, ESXi hosts go into maintenance mode and the Distributed Resource Scheduler might trigger mass migration of VMs. As a result, vSphere vMotion with the Distributed Firewall rule might fail on some VMs and cause the DFW rule to be detached from the host.

This issue is resolved in this release.

PR 3477772: Encrypted virtual machines with active Change Block Tracking (CBT) might intermittently power off after a rekey operation

Due to a race condition between the VMX and hostd services for a specific VMcrypt-related reconfiguration, encrypted VMs with active CBT might unexpectedly power off during a rekey operation.

This issue is resolved in this release.

PR 3469639: Logging stops on all log files and configured remote host targets on ESXi hosts and hosts might become unresponsive

A rare deadlock situation in the ESXi log daemon vmsyslogd might cause logging to stop on all log files and configured remote host targets on ESXi hosts. As a result, the hosts might become unresponsive. The issue might occur as the result of multiple syslog reloads.

This issue is resolved in this release.

PR 3458045: ESXi hosts intermittently fail with purple diagnostic screen due to a rare race condition

A very rare race condition might lead to accessing an interface address while it is freed from another context. As a result, ESXi hosts might intermittently fail with purple diagnostic screen and an error such as `#PF Exception 14 in world 1001391810:dhclient-uw IP 0x420003562680`.

This issue is resolved in this release.

PR 3398458: ESXi hosts become unresponsive due to pointer blocks cached filling VMFS heap to its limit

Copies of pointer blocks that are part of data transactions between ESXi hosts might be cached in the VMFS heap even after the transactions are completed. Such cached pointer blocks might fill in the heap to its limit and as a result, ESXi hosts become unresponsive from vCenter and eventually virtual machines might go offline.

This issue is resolved in this release.

PR 3390998: ESXi hosts might fail with a purple diagnostic screen due to an incomplete cleanup of a SCSI path after deleting a controller

If a controller is deleted before a device claim process completes, the `namespace` object is removed, but the SCSI Path object remains. When adding a new `namespace`, the SCSI Path might prematurely become claimable, leading to a partially populated `PsaNvmePath` object. If a claim thread picks up that path before initialization, the ESXi host might fail with a purple diagnostic screen with an error such as:`@BlueScreen: #PF Exception 14 in world 1001448541:Cmpl-vmhba66 IP 0x420025354538 addr 0x0`.

This issue is resolved in this release.

PR 3358960: In the vmkernel logs, you see multiple errors from the network interface drivers for an unsupported feature

When the ESXi NetQueue load balancer, which uses load balancing algorithms to manage the vNIC and VMkernel adapter filters, sends a VMK_UPLINK_QUEUE_FEAT_LATENCY request to a nmlx5 driver, you see multiple errors in the vmkernel logs. VMK_UPLINK_QUEUE_FEAT_LATENCY is a software queue feature and if a client request contains this feature, the NIC drivers do not allocate queues but log errors that an unregistered feature is requested.

This issue is resolved in this release. The fix masks VMK_UPLINK_QUEUE_FEAT_LATENCY in requests for queue allocation from NIC drivers.

PR 3441399: You cannot upload virtual machine template of version ESXi 7.0 Update 3 with a DirectPath I/O device to the Content Library

When you create a template from an ESXi 7.0 Update 3 VM with a DirectPath I/O device, the upload to the Content Library fails with a `Null Pointer` exception. In the vSphere Client, you see an error such as `Failed to export OVF package. ThrowableProxy.cause A general runtime error occurred. An error occurred: java.lang.NullPointerException` . In the `cls.log` , you see the error `java.lang.NullPointerException: null` .

This issue is resolved in this release.

PR 3393549: Windows and Citrix virtual machines with vGPU intermittently fail with driver-related blue diagnostic screen

Windows and Citrix VMs with a vGPU device might intermittently run out of file handles and fail with a blue diagnostic screen.

This issue is resolved in this release. The fix allows you to increase the number of file handles to 16384 for Windows and Citrix VMs with a vGPU device. For more information, see KB 369633.

PR 3434172: You cannot apply a reverse path filter for virtual machines in promiscuous mode even though /Net/ReversePathFwdCheckPromisc is active

In very specific conditions, after an upgrade of a distributed virtual switch or uninstalling an NSX transport node on an ESXi host with converged distributed virtual switch that contains a port group with active promiscuous mode, you might see some networking issues, including:

1. You cannot apply a reverse path filter for virtual machines in promiscuous mode even though **/Net/ReversePathFwdCheckPromisc** is active.
2. Intermittent packet connectivity issues when using promiscuous mode on a distributed virtual switch with multiple uplinks.

This issue is resolved in this release.

PR 3420117: ESXi hosts become non-responding during a failover

In a failover task, ESXi sends the `INQUIRY page-83` command to the target host to get port parameters but in a ghost LUN configuration some target arrays might provide unformatted output for this command. As a result, the failover task fails and in the kernel logs you see the message `Target completed the Inquiry VPD Page 0x83 request with good status but returned junk data` .

This issue is resolved in this release.

PR 3437311: The intrusion detection and prevention system (IDS/IPS) might report false positives for dropped packets in vSphere reporting tools

In environments with active IDS/IPS, ESXi might report false positives for dropped packets to network monitoring solutions such as Aria Operations. If you deactivate IDS/IPS, the count of dropped packets falls. The issue affects all virtual machines connected to NSX segments.

This issue is resolved in this release.

PR 3398462: Virtual machines residing on a vSphere Virtual Volumes datastore might become inaccessible due to a size reporting issue

An issue in the VASA provider might report an inflated size for the home directory that contains metadata files for a virtual machine and VMFS automatically expands to accommodate the larger size. However, if the VASA provider later reports the correct size, VMFS cannot shrink, and the home directory cannot open. As a result, all VM files stored in the home folder become inaccessible and you cannot access the VMs.

This issue is resolved in this release.

PR 3407529: Virtual machines with snapshots and active encryption experience higher I/O latency

In rare cases, encrypted VMs with snapshots might experience higher than expected latency. This issue occurs due to unaligned I/O operations that generate excessive metadata requests to the underlying storage and lead to increased latency.

This issue is resolved in this release. To optimize performance, the VMcrypt I/O filter is enhanced to allocate memory in 4K-aligned blocks for both read and write operations. This reduction in metadata overhead significantly improves overall I/O performance.

PR 3410295: You see gaps in the collection of metrics for some virtual machines

Due to a time sync issue, collection of data for some VMs might fail and you do not see any performance data in platforms such as Aria Operations. In the */var/run/log/vobd.log* on the ESXi host, you see errors such as: `1149:2024-06-11T05:01:11.250Z: [ClockCorrelator] 7826272852729us: [vob.clock.correction.adjtime.sync] system clock synchronized to upstream time servers`

This issue is resolved in this release. The fix caches results from Stats Registry queries with selected dynamic counters to make sure metrics are consistent.

PR 3401554: vSAN Original Storage Architecture (OSA) virtual machines with large-sized VMDKs might experience performance degradation or become inaccessible

In vSAN OSA environments of version 8.0 and later, VMDK objects with a large amount of used capacity, such as close to the maximum of 62 TB, might overload the scrubber, which leads to a race condition that might cause such objects to experience performance degradation or become inaccessible.

This issue is resolved in this release.

PR 3359530: ESXi hosts fail with purple diagnostic screen due to a pNIC driver memory overload

In a rare situation when memory-intensive workloads that fragment system memory run in parallel with throughput-intensive workloads on a virtual switch configured with 9000 MTU or more, ESXi hosts might fail with a purple diagnostic screen. As a result, power-on virtual machines become temporarily unavailable. The issue occurs because memory allocation requests from the pNIC driver overload the memory subsystem with a growing networking packet heap, which causes ESXi to fail with a stack trace at `/var/cores/` such as:

```
NMI_Interrupt@vmkernel#nover+0x561
IDTNMIWork@vmkernel#nover+0x7f
Int2_NMI@vmkernel#nover+0x19
gate_entry@vmkernel#nover+0x68
Timer_GetCycles@vmkernel#nover+0x2
SP_WaitLockIRQ@vmkernel#nover+0xd5
SPLockIRQWork@vmkernel#nover+0x3e
Heap_AlignWithTimeoutAndRA@vmkernel#nover+0xea
Pkt_AllocHandleWithSize@vmkernel#nover+0x165
Pkt_AllocWithFlags@vmkernel#nover+0xd
vmk_PktAllocForDMAEngine@vmkernel#nover+0x46
```

This issue is resolved in this release. With the fix, you can reserve enough memory for the pNIC driver using the command `esxcli system settings kernel set -s netPktJumboSlabMinSize -v <MEMORY_SIZE_TO_RESERVE_IN_MB>`. To define the amount of memory you need to reserve, use this formula: `reservation size = (numPnics * numRxQueues * (rxRingSize + 64) + numPcpus *256) * 10KB`. For example, for an ESXi host with 72 PCPUs and 4 PNICs with 10 queues of ring size set to 4K each, the reservation is about 2048 MB.

PR 3400360: VMFS6 automatic UNMAP feature might fail to reclaim filesystem space beyond 250GB

In certain cases, when you delete a filesystem space of more than 250GB on a VMFS6 volume, for example 1 TB, if the volume has no active references such as active VMs, then the VMFS6 automatic UNMAP feature might fail to reclaim the filesystem space beyond 250GB.

This issue is resolved in this release.

PR 3355390: An ESXi host fails with a purple diagnostic screen and message @BlueScreen: NMI IPI: Panic requested by another PCPU

If firewall rules in your environment result in packets moving across multiple portsets, a race condition might cause software locks to end in a deadlock. As a result, an ESXi host might fail with a purple diagnostic screen and message `@BlueScreen: NMI IPI: Panic requested by another PCPU`.

This issue is resolved in this release.

PR 3404507: ESXi hosts might fail with purple diagnostic screen due to a rare memory allocation error

If a VM power-on fails, a function that allocates memory on the heap might not free certain allocations and cause a memory leak. As a result, the ESXi host fails with a purple diagnostic screen in `World_DestroyHeap` with `NOT_IMPLEMENTED bora/vmkernel/main/world.c:2293` and `Unable to complete wait for non-empty heap` errors.

This issue is resolved in this release. The fix makes sure a cleanup function runs to free allocations to prevent the issue.

PR 3406156: Extracting a vSphere Lifecycle Manager image from an existing ESXi host might fail after a kernel configuration change

Each update of the kernel configuration also triggers an update to the `/bootbank/useropts.gz` file, but due to a rare issue, the `basemisc.tgz` might not contain the default `useropts` file after such an update. As a result, when attempting to extract a vSphere Lifecycle Manager image from an existing ESXi host, the absence of the default `useropts` file leads to failure to create the `esx-base.vib` file and the operational also fails.

This issue is resolved in this release.

PR 3396464: A lost cleanup callback might cause purple diagnostic screen failures in vSAN clusters with Remote Direct Memory Access (RDMA)

In Express Storage Architecture (ESA) vSAN clusters with active RDMA, a rare issue with a lost cleanup callback might cause a purple diagnostic screen failure with a message such as `Failed to wait for object exit`. The issue is specific to RDMA use in vSAN.

This issue is resolved in this release.

PR 3398279: Creating a vSAN File Service fails when you use IPs within the 172.17.0.0/16 range as mount points

Prior to vSphere 7.0 Update 3v, you must change your network configuration in cases when the specified file service network overlaps with the Docker default internal network 172.17.0.0/16. As a result, in the network configuration step of the File Service activation workflow, when you enter a subnet with 172.17.**.**, you see a warning and you cannot create vSAN File Services.

This issue is resolved in this release. The fix routes traffic to the correct endpoint to avoid possible conflicts. The fix is in the vSAN File Service Virtual Machine, and if you upgrade the file service to 7.0 Update 3v, you can ignore the conflict warning and continue the file service activation with subnet 172.17.0.0/16.

PR 3365863: ESXi hosts might fail with a purple diagnostic screen during high volume of outstanding I/O requests combined with slow storage performance

Under heavy I/O loads, a bug in the ESXi storage stack can cause an ESXi host to fail with a purple diagnostics screen if the storage cannot process the I/O requests quickly and some virtual machines on the ESXi host start issuing I/O resets.

This issue is resolved in this release.

PR 3332717: An ESXi hosts might fail with a purple diagnostic screen during a file close on a NFS41 datastore

A file close on a NFS41 datastore might lead to memory corruption in a layer common across file systems. A subsequent file open on an NFSv3 datastore picks up the same memory zone. As a result, the ESXi host might fail with a purple diagnostic screen with a backtrace similar to:

```
NFSDestroySchedQueue NFS
Sched_DestroySchedQueue
NFSVolume_DestroySchedQHandle
```

This issue is resolved in this release.

PR 3352007: ESXi hosts might fail with a purple diagnostics screen and with errors for CpuSchedWait() and FS3_ReportCorruption() in the backtrace

In a data corruption scenario, the corruption report routine requires to load the VMFS datastore volume header metadata and perform a validation. In very rare cases, a spinlock might prevent reading this metadata and as a result, ESXi hosts might fail with a purple diagnostics screen. In the backtrace, you see errors for `CpuSchedWait()` and `FS3_ReportCorruption()`.

This issue is resolved in this release. The fix enhances the data corruption report routine to allow skipping the read on the volume header metadata for such rare cases.

PR 3367834: A fault tolerance secondary virtual machine might restart by accident

In very rare cases, a fault tolerance secondary VM might restart unexpectedly while other fault tolerance VMs power off or migrate from the ESXi host.

This issue is resolved in this release.

PR 3389767: During a vSphere vMotion migration of a fault tolerant Primary VM with encryption, the migration task might fail and vSphere FT failover occurs

In rare cases, the encryption key package might not be sent or received correctly during a vSphere vMotion migration of a fault tolerant Primary VM with encryption, and as a result the migration task fails and vSphere FT failover occurs.

This issue is resolved in this release. The fix sends the encryption key at the end of the vSphere FT checkpoint to avoid errors.

PR 3382561: Virtual machines that share the same encryption key are randomly locked after the ESXi host reboots

When cloned from a single VM, several VMs can share the same encryption key. After an ESXi host reboot, each key of such VMs is added to the key cache, but while the first key addition succeeds, subsequent additions fail because the key already exists in the cache, and the key is removed. As a result, such VMs become locked.

This issue is resolved in this release.

esx-update_7.0.3-0.145.24723872

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes

Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.145.24723872 • VMware_bootbank_esx-update_7.0.3-0.145.24723872
PRs Fixed	3422040, 3412449, 3400844, 3365671
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs to resolve the following issue:

PR 3412449: Remediation of ESXi hosts might fail due to a timeout in the update of the VMware-VM-Tools component

While upgrading ESXi hosts by using vSphere Lifecycle Manager, remediation of the VMware-VM-Tools component might occasionally fail due to a timeout. The issue occurs when the update process takes longer than the timeout setting of 30 sec for the VMware-VM-Tools component.

This issue is resolved in this release. The fix increases the timeout limit to 120 sec.

Broadcom-ntg3_4.1.15.0-4vmw.703.0.145.24723872

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_ntg3_4.1.15.0-4vmw.703.0.145.24723872
PRs Fixed	3411044
CVE numbers	N/A

Updates the `ntg3` VIB to resolve the following issue:

PR 3411044: ESXi host might lose network connectivity due to a very rare issue with the ntg3 driver

A data race in the handling of tx queue full situation in the ntg3 driver might cause in very rare cases the TX queue to stop transmitting packets. As a result, you see either virtual machines or ESXi host management network, or both, lose connectivity. In the vmkernel log of the affected ESXi host, you see messages such as `Uplink: XXXX: Queue 0 of device vmnicX stuck, resetting the device` and/or `Vmxnet3: XXXXX: XXXX, portID(XXXXX): Hang detected.`

This issue is resolved in this release. The fix is part of ntg3 4.1.15.

VMware-NVMeoF-TCP_1.0.0.7-1vmw.703.0.145.24723872

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A

Affected Software	N/A
Affected VIBs	• VMW_bootbank_nvmetcp_1.0.0.7-1vmw.703.0.145.24723872
PRs Fixed	3437679, 3414590, 3364569
CVE numbers	N/A

Updates the `nvmetcp` VIB to resolve the following issues:

PR 3414590: Snapshot tasks on virtual machines on NVMe/TCP datastores might take much longer than on VMs provisioned on NVMe/FC datastores

When creating or deleting a snapshot on a VM provisioned on datastores backed by NVMe/TCP namespaces, such tasks might take much longer than on VMs provisioned on datastores backed by NVMe/FC namespaces. The issue occurs because the nvmetcp driver handles some specific NVMe commands not in the way the NVMe/TCP target systems expect.

This issue is resolved in this release.

PR 3437679: ESXi host fails with a purple diagnostic screen due to mishandling a canceled NVMe write command

In rare cases, a large-size NVMe write command might be canceled due to an I/O timeout but the nvmetcp driver might again complete the command and this causes the ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3364569: If a NVMe/TCP driver fails to process an I/O command, an ESXi host might disconnect from a storage array

If your ESXi hosts connect to storage arrays and perform read/write operations by using NVMe/TCP connections, when a NVMe/TCP driver fails to process an I/O command, ESXi might cancel the process with an abort command. As a result, an ESXi host might disconnect from a storage array and end previous I/O queues.

This issue is resolved in this release.

ESXi_7.0.3-0.140.24723868

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_bmcal_7.0.3-0.140.24723868 • VMware_bootbank_trx_7.0.3-0.140.24723868 • VMware_bootbank_esxio-combiner_7.0.3-0.140.24723868 • VMware_bootbank_esx-xserver_7.0.3-0.140.24723868 • VMware_bootbank_vsan_7.0.3-0.140.24723868 • VMware_bootbank_native-misc-drivers_7.0.3-0.140.24723868 • VMware_bootbank_gc_7.0.3-0.140.24723868 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.140.24723868 • VMware_bootbank_vdfs_7.0.3-0.140.24723868 • VMware_bootbank_crx_7.0.3-0.140.24723868 • VMware_bootbank_vsanhealth_7.0.3-0.140.24723868 • VMware_bootbank_cpu-microcode_7.0.3-0.140.24723868

	• VMware_bootbank_esx-base_7.0.3-0.140.24723868
PRs Fixed	3452679, 3488111, 3456430, 3450561, 3482267, 3479599, 3484230, 3476566, 3452717, 3432584, 3475105, 3470206, 3452699, 3435458, 3404661, 3400981, 3444626, 3469216, 3454671, 3469563, 3457662, 3447985, 3443017, 3432572, 3432690, 3404668, 3430751, 3400984, 3406922, 3430750, 3406923, 3425364, 3398141, 3406188, 3400967, 3430766, 3316536, 3408358, 3408125, 3390665, 3411970, 3412457, 3400130, 3404669, 3386280
CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

This patch updates the `bmcal`, `trx`, `esxio-combiner`, `esx-xserver`, `vsan`, `native-misc-drivers`, `gc`, `esx-dvfilter-generic-fastpath`, `vdfs`, `crx`, `vsanhealth`, `cpu-microcode`, and `esx-base` VIBs to resolve the following issues:

ESXi 7.0 Update 3v includes the following Intel microcode:

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	baseline	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	baseline	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	baseline	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	baseline	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	baseline	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	baseline	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	baseline	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	baseline	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	baseline	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	baseline	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	baseline	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	baseline	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	baseline	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Haswell EP	0x306f2 (06/3f/2)	0x6f	baseline	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	baseline	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	baseline	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	baseline	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	baseline	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	baseline	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	baseline	0x4003801	8/1/2024	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	baseline	0x5003801	8/1/2024	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	baseline	0x7002a01	8/1/2024	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	baseline	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	baseline	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	baseline	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	baseline	0xe000015	8/3/2023	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	baseline	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	baseline	0x3e	10/5/2023	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	baseline	0xd0003f5	8/2/2024	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	baseline	0x10002c0	8/8/2024	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	baseline	0x4c000026	2/28/2024	Intel Atom P5000 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Snow Ridge	0x80667 (06/86/7)	0x01	baseline	0x4c000026	2/28/2024	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	baseline	0xba	8/1/2024	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	baseline	0x3a	8/1/2024	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	baseline	0x54	8/1/2024	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	baseline	0x2c0003e0	7/30/2024	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	baseline	0x2b000620	7/30/2024	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	baseline	0xf8	9/28/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/ a)	0x22	baseline	0xfa	7/28/2024	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/ b)	0x02	baseline	0xf6	2/1/2024	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	baseline	0xf8	2/1/2024	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/ d)	0x22	baseline	0x102	7/31/2024	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/ a7/1)	0x02	baseline	0x63	8/1/2024	Intel Xeon E-2300 Series
Raptor Lake E/ HX/S	0xb0671 (06/ b7/1)	0x32	baseline	0x12c	9/25/2024	Intel Xeon E-2400 Series
Emerald Rapids SP	0xc06f2 (06/cf/2)	0x87	baseline	0x21000291	7/30/2024	Intel Xeon 8500 Series; Intel Xeon Gold 6500/5500 Series; Intel Xeon Silver 4500 Series; Intel Xeon Bronze 3500 Series

PR 3408358: Security scans on ESXi hosts with OpenSSH 8.8 show multiple CVEs

When for some reason you need to activate OpenSSH on an ESXi host, if the OpenSSH version is 8.8 and you run a security scan, you might see multiple CVEs.

This issue is resolved in this release. The fix updates OpenSSH to version 9.3p2 and backports security fixes from later versions: CVE-2024-6387, CVE-2023-51385, CVE-2023-51384, CVE-2023-48795, CVE-2023-38408. The version string is updated to **OpenSSH_9.3p2 vmw9.8p1** to indicate the backported patches.

esx-update_7.0.3-0.140.24723868

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_esx-update_7.0.3-0.140.24723868 • VMware_bootbank_loadesx_7.0.3-0.140.24723868
PRs Fixed	N/A
CVE numbers	N/A

This patch updates the `esx-update` and `loadesx` VIBs.

VMware-VM-Tools_12.5.1.24649672-24723868

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_locker_tools-light_12.5.1.24649672-24723868
PRs Fixed	3494213, 3409318
CVE numbers	N/A

This patch updates the `tools-light` VIB:

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3v:

- **windows.iso**: VMware Tools 12.5.1 supports the following 64-bit Windows versions:- Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  For **windows.iso** support for 32-bit Windows versions: Windows 7 SP1 or Windows Server 2008 R2 SP1 and later, refer to VMware Tools 12.4.5 Release Notes.
  VMware Tools 12.5.0 provides support for Windows Server 2025, but make sure your system supports Windows 2025 if you plan to use Windows 2025 as a guest OS on virtual machines. For more information, see Installing Windows Server 2025 on a VMware Virtual Machine.
- **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  – **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).

- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. For more details, see VMware knowledge base article 88698.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- Updating VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- What Every vSphere Admin Must Know About VMware Tools
- Earlier versions of VMware Tools
- VMware Tools 12.5.1 Release Notes

ESXi-7.0U3v-24723872-standard

Profile Name	ESXi-7.0U3v-24723872-standard
Build	For build information, see the Patches Contained in This Release section.
Vendor	Broadcom, Inc.
Release Date	May 20, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_native-misc-drivers_7.0.3-0.145.24723872 • VMware_bootbank_vsan_7.0.3-0.145.24723872 • VMware_bootbank_bmcal_7.0.3-0.145.24723872 • VMware_bootbank_esx-xserver_7.0.3-0.145.24723872 • VMware_bootbank_gc_7.0.3-0.145.24723872 • VMware_bootbank_esx-base_7.0.3-0.145.24723872 • VMware_bootbank_esxio-combiner_7.0.3-0.145.24723872 • VMware_bootbank_trx_7.0.3-0.145.24723872 • VMware_bootbank_cpu-microcode_7.0.3-0.145.24723872 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.145.24723872 • VMware_bootbank_vsanhealth_7.0.3-0.145.24723872 • VMware_bootbank_crx_7.0.3-0.145.24723872 • VMware_bootbank_vdfs_7.0.3-0.145.24723872 • VMware_bootbank_loadesx_7.0.3-0.145.24723872 • VMware_bootbank_esx-update_7.0.3-0.145.24723872 • VMW_bootbank_ntg3_4.1.15.0-4vmw.703.0.145.24723872 • VMW_bootbank_nvmetcp_1.0.0.7-1vmw.703.0.145.24723872 • VMware_locker_tools-light_12.5.1.24649672-24723868
PRs Fixed	3406035, 3477734, 3489859, 3352051, 3457552, 3485174, 3469639, 3470731, 3485586, 3484794, 3484793, 3484786, 3477773, 3469106, 3477257, 3476746, 3475049, 3454755, 3469189, 3466996, 3458045, 3435833, 3447991, 3443815, 3432572, 3432690, 3441101, 3404668, 3434172, 3437311,

	3371201, 3367834, 3398462, 3410295, 3390998, 3398458, 3388843, 3398467, 3430801, 3408807, 3420117, 3417327, 3423849, 3417227, 3417328, 3404126, 3408129, 3408008, 3408126, 3398534, 3400360, 3406033, 3398361, 3398279, 3407212, 3411695, 3396010, 3412537, 3352007, 3404202, 3402976, 3396464, 3407529, 3408143, 3336865, 3403867, 3389767, 3366075, 3365863, 3404507, 3403906, 3405760, 3401554, 3398537, 3355390, 3359530, 3393549, 3367426, 3359386, 3382561, 3358960, 3422040, 3412449, 3400844, 3365671, 3411044, 3437679, 3414590, 3364569
Related CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

This patch updates the following issues:

PR 3425364: Setting `cloud-init guestInfo` variables by regular users in the guest results into an error

Starting with ESXi 7.0 Update 3v, setting `cloud-init guestInfo` variables by regular users in the guest results into an error due to design changes.

This issue is resolved in this release. For more information, see KB 377267.

PR 3406033: ESXi host fails with a purple diagnostic screen due to a rare physical CPU (PCPU) lockup

In the vSphere Client, when you use the **Delete from Disk** option to remove a virtual machine from a vCenter system and delete all VM files from the datastore, including the configuration file and virtual disk files, if any of the files is corrupted, a rare issue with handling corrupted files in the delete path might lead to a PCPU lockup. As a result, the ESXi host fails with a purple diagnostic screen and a message such as `NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release.

PR 3484786: ESXi installation on an iSCSI LUN fails as the ESXi iSCSI Boot Firmware Table (iBFT) module fails to discover the LUN

In some cases, the iBFT control structure might have an optional expansion for which the ESXi vmkibft module doesn't have a proper check. As a result, iSCSI LUN discovery by using iBFT might fail and cause failure of the ESXi installation on the iSCSI LUN.

This issue is resolved in this release.

PR 3423217: You see vendor name of some Solidigm NVMe devices as Unknown

In the ESXi Host Client, under **Manage > Hardware > PCI Devices**, and in the vSphere Client, under **Host > Configure > Hardware > PCI Devices > All PCI Devices**, you might see the vendor name of some Solidigm NVMe devices as `Unknown`.

This issue is resolved in this release.

PR 3398537: ESXi host fails with a purple diagnostic screen due to an I/O race with an error PSOD @BlueScreen: ASSERT bora/lib/misc/bitvector.c:632

Due to a rare I/O race condition on virtual machines backed by a vSphere Virtual Volume, the ESXi host might fail with a purple diagnostic screen and an error such as `PSOD @BlueScreen: ASSERT bora/lib/misc/bitvector.c:632`.

This issue is resolved in this release.

PR 3371201: The hostd service might generate core dumps during upgrade from ESXi 6.7 to 7.x when SNMP traps are configured

In very rare cases, a missing SNMP port value when SNMP traps are configured during an upgrade from ESXi 6.7 to 7.x, might lead to hostd core dumps.

This issue is resolved in this release.

PR 3352051: Syslog configuration changes in a host profile that you use to provision ESXi host with Auto Deploy stateful install do not persist across reboots

If you change the syslog configuration of a host profile and provision ESXi hosts with that profile by using the Auto Deploy stateful install, changes might not persist after the hosts reboot.

This issue is resolved in this release.

PR 3396010: Controller VMs with direct I/O devices in third-party hyper converged infrastructure environments experience guest kernel soft lockups

A rare race condition between the interrupt virtualization and the VMkernel CPU scheduler in an ESXi host might result in guest kernel soft lockups on controller VMs with direct I/O devices in third-party hyper converged infrastructure environments. The soft locks cause virtual machines in the entire cluster to lose NFS storage connectivity and I/O access.

This issue is resolved in this release.

PR 3359386: If the Latency Sensitivity parameter of a virtual machine is set to High, you cannot add memory to that VM when powered off

If you use the vSphere Client to set the `Latency Sensitivity` parameter of a VM to `High` , attempts to add memory to such a VM when powered off might fail with an error such as `A specified parameter was not correct: spec.memoryAllocation` .

This issue is resolved in this release.

PR 3403867: Setting the CPU limit to 0 makes virtual machines unresponsive

If for any reason you set the CPU limit of running virtual machines to `0` , this causes CPU starvation and the VMs become unresponsive.

This issue is resolved in this release.

PR 3457552: You might see multiple hardware sensor alerts due to a Baseboard Management Controller (BMC) issue

An underlying BMC issue might cause ESXi hardware health monitoring to produce multiple alerts for hardware sensors on ESXi hosts, which you see in the vSphere Client under **Monitor > Tasks and Events**.

This issue is resolved in this release. The fix logs raw sensor data directly from IPMI to provide a data point to debug possible BMC issues that cause false alerts but cannot prevent BMC issues from occuring.

PR 3484794: Restoring the iSCSI configurations on an ESXi host might fail during boot due to stale entries in the ConfigStore database

If the ConfigStore database on an ESXi host has stale iSCSI configurations related to hardware iSCSI adapters, the iSCSI jumpstart might fail and restoring the iSCSI configuration on that host also fails during boot.

This issue is resolved in this release.

PR 3484793: Discovery of iSCSI dynamic targets, LUNs, and datastores fails on ESXi host reboot

In some cases, dynamic discovery of targets in systems that use dynamic discovery addresses for iSCSI configuration might fail. As a result, you do not see iSCSI targets, LUNs, and datastores after a reboot of ESXi hosts. The dynamic discovery of iSCSI targets might also fail when the Challenge-Handshake Authentication Protocol (CHAP) is active on the ESXi host.

This issue is resolved in this release.

PR 3458283: A rare Baseboard Management Controller (BMC) issue might cause some applications to become unresponsive

If an application sends an IPMI request to the BMC while it resets, such requests remain indefinitely pending and cause the applications to become unresponsive.

This issue is resolved in this release. The fix updates the IPMI driver to handle such conditions.

PR 3485174: Guest OS might mark file system read-only after repeated I/O failure which can cause Kubernetes control plane nodes to go into Read-only mode

An issue with the check for max allowed memory address in memory mapping code during I/O processing at virtual SCSI might cause a guest OS on an ESXi host to mark guest file system as read-only. As a result, Kubernetes control plane nodes might go into Read-only mode. In the vmkernel logs, you see multiple error messages such as `failed to pin: I/O error.`

This issue is resolved in this release.

PR 3470731: Unsupported SCSI Read Mode Sense Page commands to a Raw Disk Mapping (RDM) target might cause virtual machines to become unresponsive

A large number of unsupported SCSI Read Mode Sense Page commands to a RDM target from a VM configured with an RDM device might exceed the storage heap and cause both the datastore and the VM to become unresponsive.

This issue is resolved in this release. The fix prevents blocking VM I/O operations by optimizing the handling of unsupported SCSI commands or mode pages. Specifically, in passthrough mode used for RDM devices, the system no longer attempts to process such unsupported commands in a way that consumes storage heap resources.

PR 3398467: vSphere Virtual Volumes daemon fails after converting a VASA provider from external to internal

Due to an issue with handling IDs during an unbind operation for some vSphere API for Storage Awareness (VASA) providers, in some tasks such as converting a VASA provider from external to internal, the vSphere Virtual Volumes daemon vvold might fail as it cannot map unique IDs.

This issue is resolved in this release. With the fix, vvold gracefully handles such conditions and stops the unbind operation with message in the logs instead of failing.

PR 3414590: Snapshot tasks on virtual machines on NVMe/TCP datastores might take much longer than on VMs provisioned on NVMe/FC datastores

When creating or deleting a snapshot on a VM provisioned on datastores backed by NVMe/TCP namespaces, such tasks might take much longer than on VMs provisioned on datastores backed by NVMe/FC namespaces. The issue occurs because the nvmetcp driver handles some specific NVMe commands not in the way the NVMe/TCP target systems expect.

This issue is resolved in this release.

PR 3388843: You cannot activate Kernel DMA Protection on a virtual machine with Windows OS and Intel processor

When virtual Input-Output Memory Management Unit (vIOMMU) is active on a virtual machine with Windows OS and an Intel CPU, you might not be able to activate Kernel DMA Protection.

This issue is resolved in this release. The fix adds `acpi.dmar.enableDMAProtection=TRUE` to the vmx advanced settings that you can use if required.

PR 3469106: ESXi hosts intermittently disconnect from the Active Directory domain or from vCenter

Memory leaks might occur in Likewise during Active Directory operations or if smart card authentication is active on an ESXi host. As a result, Likewise processes might run out of memory and ESXi hosts intermittently disconnect from the Active Directory domain or from vCenter. In the `/var/log/vmkernel.log` file, you see messages similar to:

```
yyyy-mm-dd In(182) vmkernel: cpu72:2110465)uw.2110464 (44739) requires 1024 KB, asked 1024 KB from likewise (792) which has 93112 KB occupied and 72 KB available.
```

```
yyyy-mm-dd In(182) vmkernel: cpu72:2110465)Admission failure in path: host/vim/vmvisor/likewise:lwsmd.2110464:uw.2110464
```

In the `hostd-probe.log` file you see a message such as: `hostd detected to be non-responsive.`

This issue is resolved in this release. The fix adds a system service that monitors Likewise memory usage and restarts relevant services in case memory consumption approaches Likewise limits.

PR 3477734: ESXi host fails with a purple diagnostic screen while activating HClock

If for some reason an ESXi host fails to allocate memory for the activation of the HClock capability, the error handling goes into CPU wait state while it still holds a lock. As a result, the host fails with a purple diagnostic screen, and you see backtraces such as:

```
[0x2b8c]RCU_WaitForGracePeriod@vmkernel#nover stack:
[0xa000]vmk_HashRelease@vmkernel#nover+ stack:
[0xa0000]NetSchedHClkConnect@(netsched_hclk)#<None> stack:
```

This issue is resolved in this release.

PR 3489859: Migration of virtual machines fails with an error "Failed to allocate migration heap" on the source ESXi host

In very rare cases, if a virtual machine powers off before a running migration completes, ESXi might fail to clean up the migration heap. If the memory leak continues over time, the migration heap might be exhausted, and virtual machines cannot migrate from such ESXi hosts.

This issue is resolved in this release.

PR 3499302: If a virtual machine migrates to an ESXi host undergoing NSX update, the Distributed Firewall rule might be detached from that host

During NSX update or upgrade, ESXi hosts go into maintenance mode and the Distributed Resource Scheduler might trigger mass migration of VMs. As a result, vSphere vMotion with the Distributed Firewall rule might fail on some VMs and cause the DFW rule to be detached from the host.

This issue is resolved in this release.

PR 3477772: Encrypted virtual machines with active Change Block Tracking (CBT) might intermittently power off after a rekey operation

Due to a race condition between the VMX and hostd services for a specific VMcrypt-related reconfiguration, encrypted VMs with active CBT might unexpectedly power off during a rekey operation.

This issue is resolved in this release.

PR 3469639: Logging stops on all log files and configured remote host targets on ESXi hosts and hosts might become unresponsive

A rare deadlock situation in the ESXi log daemon vmsyslogd might cause logging to stop on all log files and configured remote host targets on ESXi hosts. As a result, the hosts might become unresponsive. The issue might occur as the result of multiple syslog reloads.

This issue is resolved in this release.

PR 3458045: ESXi hosts intermittently fail with purple diagnostic screen due to a rare race condition

A very rare race condition might lead to accessing an interface address while it is freed from another context. As a result, ESXi hosts might intermittently fail with purple diagnostic screen and an error such as `#PF Exception 14 in world 1001391810:dhclient-uw IP 0x420003562680`.

This issue is resolved in this release.

PR 3398458: ESXi hosts become unresponsive due to pointer blocks cached filling VMFS heap to its limit

Copies of pointer blocks that are part of data transactions between ESXi hosts might be cached in the VMFS heap even after the transactions are completed. Such cached pointer blocks might fill in the heap to its limit and as a result, ESXi hosts become unresponsive from vCenter and eventually virtual machines might go offline.

This issue is resolved in this release.

PR 3390998: ESXi hosts might fail with a purple diagnostic screen due to an incomplete cleanup of a SCSI path after deleting a controller

If a controller is deleted before a device claim process completes, the `namespace` object is removed, but the SCSI Path object remains. When adding a new `namespace` , the SCSI Path might prematurely become claimable, leading to a partially populated `PsaNvmePath` object. If a claim thread picks up that path before initialization, the ESXi host might fail with a purple diagnostic screen with an error such as:`@BlueScreen: #PF Exception 14 in world 1001448541:Cmpl-vmhba66 IP 0x420025354538 addr 0x0` .

This issue is resolved in this release.

PR 3358960: In the vmkernel logs, you see multiple errors from the network interface drivers for an unsupported feature

When the ESXi NetQueue load balancer, which uses load balancing algorithms to manage the vNIC and VMkernel adapter filters, sends a VMK_UPLINK_QUEUE_FEAT_LATENCY request to a nmlx5 driver, you see multiple errors in the vmkernel logs. VMK_UPLINK_QUEUE_FEAT_LATENCY is a software queue feature and if a client request contains this feature, the NIC drivers do not allocate queues but log errors that an unregistered feature is requested.

This issue is resolved in this release. The fix masks VMK_UPLINK_QUEUE_FEAT_LATENCY in requests for queue allocation from NIC drivers.

PR 3441399: You cannot upload virtual machine template of version ESXi 7.0 Update 3 with a DirectPath I/O device to the Content Library

When you create a template from an ESXi 7.0 Update 3 VM with a DirectPath I/O device, the upload to the Content Library fails with a `Null Pointer` exception. In the vSphere Client, you see an error such as `Failed to export OVF package. ThrowableProxy.cause A general runtime error occurred. An error occurred: java.lang.NullPointerException` . In the `cls.log` , you see the error `java.lang.NullPointerException: null` .

This issue is resolved in this release.

PR 3437679: ESXi host fails with a purple diagnostic screen due to mishandling a canceled NVMe write command

In rare cases, a large-size NVMe write command might be canceled due to an I/O timeout but the nvmetcp driver might again complete the command and this causes the ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3393549: Windows and Citrix virtual machines with vGPU intermittently fail with driver-related blue diagnostic screen

Windows and Citrix VMs with a vGPU device might intermittently run out of file handles and fail with a blue diagnostic screen.

This issue is resolved in this release. The fix allows you to increase the number of file handles to 16384 for Windows and Citrix VMs with a vGPU device. For more information, see KB 369633.

PR 3434172: You cannot apply a reverse path filter for virtual machines in promiscuous mode even though /Net/ ReversePathFwdCheckPromisc is active

In very specific conditions, after an upgrade of a distributed virtual switch or uninstalling an NSX transport node on an ESXi host with converged distributed virtual switch that contains a port group with active promiscuous mode, you might see some networking issues, including:

1. You cannot apply a reverse path filter for virtual machines in promiscuous mode even though **/Net/ ReversePathFwdCheckPromisc** is active.
2. Intermittent packet connectivity issues when using promiscuous mode on a distributed virtual switch with multiple uplinks.

This issue is resolved in this release.

PR 3420117: ESXi hosts become non-responding during a failover

In a failover task, ESXi sends the `INQUIRY page-83` command to the target host to get port parameters but in a ghost LUN configuration some target arrays might provide unformatted output for this command. As a result, the failover task fails and in the kernel logs you see the message `Target completed the Inquiry VPD Page 0x83 request with good status but returned junk data.`

This issue is resolved in this release.

PR 3437311: The intrusion detection and prevention system (IDS/IPS) might report false positives for dropped packets in vSphere reporting tools

In environments with active IDS/IPS, ESXi might report false positives for dropped packets to network monitoring solutions such as Aria Operations. If you deactivate IDS/IPS, the count of dropped packets falls. The issue affects all virtual machines connected to NSX segments.

This issue is resolved in this release.

PR 3398462: Virtual machines residing on a vSphere Virtual Volumes datastore might become inaccessible due to a size reporting issue

An issue in the VASA provider might report an inflated size for the home directory that contains metadata files for a virtual machine and VMFS automatically expands to accommodate the larger size. However, if the VASA provider later reports the correct size, VMFS cannot shrink, and the home directory cannot open. As a result, all VM files stored in the home folder become inaccessible and you cannot access the VMs.

This issue is resolved in this release.

PR 3411044: ESXi host might lose network connectivity due to a very rare issue with the ntg3 driver

A data race in the handling of tx queue full situation in the ntg3 driver might cause in very rare cases the TX queue to stop transmitting packets. As a result, you see either virtual machines or ESXi host management network, or both, lose connectivity. In the vmkernel log of the affected ESXi host, you see messages such as `Uplink: XXXX: Queue 0 of device vmnicX stuck, resetting the device` and/or `Vmxnet3: XXXXX: XXXX, portID(XXXXX): Hang detected.`

This issue is resolved in this release. The fix is part of ntg3 4.1.15.

PR 3407529: Virtual machines with snapshots and active encryption experience higher I/O latency

In rare cases, encrypted VMs with snapshots might experience higher than expected latency. This issue occurs due to unaligned I/O operations that generate excessive metadata requests to the underlying storage and lead to increased latency.

This issue is resolved in this release. To optimize performance, the VMcrypt I/O filter is enhanced to allocate memory in 4K-aligned blocks for both read and write operations. This reduction in metadata overhead significantly improves overall I/O performance.

PR 3410295: You see gaps in the collection of metrics for some virtual machines

Due to a time sync issue, collection of data for some VMs might fail and you do not see any performance data in platforms such as Aria Operations. In the */var/run/log/vobd.log* on the ESXi host, you see errors such as: `1149:2024-06-11T05:01:11.250Z: [ClockCorrelator] 7826272852729us: [vob.clock.correction.adjtime.sync] system clock synchronized to upstream time servers`

This issue is resolved in this release. The fix caches results from Stats Registry queries with selected dynamic counters to make sure metrics are consistent.

PR 3401554: vSAN Original Storage Architecture (OSA) virtual machines with large-sized VMDKs might experience performance degradation or become inaccessible

In vSAN OSA environments of version 8.0 and later, VMDK objects with a large amount of used capacity, such as close to the maximum of 62 TB, might overload the scrubber, which leads to a race condition that might cause such objects to experience performance degradation or become inaccessible.

This issue is resolved in this release.

PR 3359530: ESXi hosts fail with purple diagnostic screen due to a pNIC driver memory overload

In a rare situation when memory-intensive workloads that fragment system memory run in parallel with throughput-intensive workloads on a virtual switch configured with 9000 MTU or more, ESXi hosts might fail with a purple diagnostic screen. As a result, power-on virtual machines become temporarily unavailable. The issue occurs because memory allocation requests from the pNIC driver overload the memory subsystem with a growing networking packet heap, which causes ESXi to fail with a stack trace at `/var/cores/` such as:

```
NMI_Interrupt@vmkernel#nover+0x561
IDTNMIWork@vmkernel#nover+0x7f
Int2_NMI@vmkernel#nover+0x19
gate_entry@vmkernel#nover+0x68
Timer_GetCycles@vmkernel#nover+0x2
SP_WaitLockIRQ@vmkernel#nover+0xd5
SPLockIRQWork@vmkernel#nover+0x3e
Heap_AlignWithTimeoutAndRA@vmkernel#nover+0xea
Pkt_AllocHandleWithSize@vmkernel#nover+0x165
Pkt_AllocWithFlags@vmkernel#nover+0xd
vmk_PktAllocForDMAEngine@vmkernel#nover+0x46
```

This issue is resolved in this release. With the fix, you can reserve enough memory for the pNIC driver using the command `esxcli system settings kernel set -s netPktJumboSlabMinSize -v <MEMORY_SIZE_TO_RESERVE_IN_MB>`. To define the amount of memory you need to reserve, use this formula: `reservation size = (numPnics * numRxQueues * (rxRingSize + 64) + numPcpus *256) * 10KB`. For example, for an ESXi host with 72 PCPUs and 4 PNICs with 10 queues of ring size set to 4K each, the reservation is about 2048 MB.

PR 3412449: Remediation of ESXi hosts might fail due to a timeout in the update of the VMware-VM-Tools component

While upgrading ESXi hosts by using vSphere Lifecycle Manager, remediation of the VMware-VM-Tools component might occasionally fail due to a timeout. The issue occurs when the update process takes longer than the timeout setting of 30 sec for the VMware-VM-Tools component.

This issue is resolved in this release. The fix increases the timeout limit to 120 sec.

PR 3400360: VMFS6 automatic UNMAP feature might fail to reclaim filesystem space beyond 250GB

In certain cases, when you delete a filesystem space of more than 250GB on a VMFS6 volume, for example 1 TB, if the volume has no active references such as active VMs, then the VMFS6 automatic UNMAP feature might fail to reclaim the filesystem space beyond 250GB.

This issue is resolved in this release.

PR 3355390: An ESXi host fails with a purple diagnostic screen and message @BlueScreen: NMI IPI: Panic requested by another PCPU

If firewall rules in your environment result in packets moving across multiple portsets, a race condition might cause software locks to end in a deadlock. As a result, an ESXi host might fail with a purple diagnostic screen and message `@BlueScreen: NMI IPI: Panic requested by another PCPU`.

This issue is resolved in this release.

PR 3404507: ESXi hosts might fail with purple diagnostic screen due to a rare memory allocation error

If a VM power-on fails, a function that allocates memory on the heap might not free certain allocations and cause a memory leak. As a result, the ESXi host fails with a purple diagnostic screen in `World_DestroyHeap` with `NOT_IMPLEMENTED bora/vmkernel/main/world.c:2293` and `Unable to complete wait for non-empty heap` errors.

This issue is resolved in this release. The fix makes sure a cleanup function runs to free allocations to prevent the issue.

PR 3406156: Extracting a vSphere Lifecycle Manager image from an existing ESXi host might fail after a kernel configuration change

Each update of the kernel configuration also triggers an update to the `/bootbank/useropts.gz` file, but due to a rare issue, the `basemisc.tgz` might not contain the default `useropts` file after such an update. As a result, when attempting to extract a vSphere Lifecycle Manager image from an existing ESXi host, the absence of the default `useropts` file leads to failure to create the `esx-base.vib` file and the operational also fails.

This issue is resolved in this release.

PR 3396464: A lost cleanup callback might cause purple diagnostic screen failures in vSAN clusters with Remote Direct Memory Access (RDMA)

In Express Storage Architecture (ESA) vSAN clusters with active RDMA, a rare issue with a lost cleanup callback might cause a purple diagnostic screen failure with a message such as `Failed to wait for object exit`. The issue is specific to RDMA use in vSAN.

This issue is resolved in this release.

PR 3398279: Creating a vSAN File Service fails when you use IPs within the 172.17.0.0/16 range as mount points

Prior to vSphere 7.0 Update 3v, you must change your network configuration in cases when the specified file service network overlaps with the Docker default internal network 172.17.0.0/16. As a result, in the network configuration step of the File Service activation workflow, when you enter a subnet with 172.17.**.**, you see a warning and you cannot create vSAN File Services.

This issue is resolved in this release. The fix routes traffic to the correct endpoint to avoid possible conflicts. The fix is in the vSAN File Service Virtual Machine, and if you upgrade the file service to 7.0 Update 3v, you can ignore the conflict warning and continue the file service activation with subnet 172.17.0.0/16.

PR 3365863: ESXi hosts might fail with a purple diagnostic screen during high volume of outstanding I/O requests combined with slow storage performance

Under heavy I/O loads, a bug in the ESXi storage stack can cause an ESXi host to fail with a purple diagnostics screen if the storage cannot process the I/O requests quickly and some virtual machines on the ESXi host start issuing I/O resets.

This issue is resolved in this release.

PR 3364569: If a NVMe/TCP driver fails to process an I/O command, an ESXi host might disconnect from a storage array

If your ESXi hosts connect to storage arrays and perform read/write operations by using NVMe/TCP connections, when a NVMe/TCP driver fails to process an I/O command, ESXi might cancel the process with an abort command. As a result, an ESXi host might disconnect from a storage array and end previous I/O queues.

This issue is resolved in this release.

PR 3332717: An ESXi hosts might fail with a purple diagnostic screen during a file close on a NFS41 datastore

A file close on a NFS41 datastore might lead to memory corruption in a layer common across file systems. A subsequent file open on an NFSv3 datastore picks up the same memory zone. As a result, the ESXi host might fail with a purple diagnostic screen with a backtrace similar to:

```
NFSDestroySchedQueue NFS
Sched_DestroySchedQueue
```

`NFSVolume_DestroySchedQHandle`

This issue is resolved in this release.

PR 3352007: ESXi hosts might fail with a purple diagnostics screen and with errors for CpuSchedWait() and FS3_ReportCorruption() in the backtrace

In a data corruption scenario, the corruption report routine requires to load the VMFS datastore volume header metadata and perform a validation. In very rare cases, a spinlock might prevent reading this metadata and as a result, ESXi hosts might fail with a purple diagnostics screen. In the backtrace, you see errors for `CpuSchedWait()` and `FS3_ReportCorruption()`.

This issue is resolved in this release. The fix enhances the data corruption report routine to allow skipping the read on the volume header metadata for such rare cases.

PR 3367834: A fault tolerance secondary virtual machine might restart by accident

In very rare cases, a fault tolerance secondary VM might restart unexpectedly while other fault tolerance VMs power off or migrate from the ESXi host.

This issue is resolved in this release.

PR 3389767: During a vSphere vMotion migration of a fault tolerant Primary VM with encryption, the migration task might fail and vSphere FT failover occurs

In rare cases, the encryption key package might not be sent or received correctly during a vSphere vMotion migration of a fault tolerant Primary VM with encryption, and as a result the migration task fails and vSphere FT failover occurs.

This issue is resolved in this release. The fix sends the encryption key at the end of the vSphere FT checkpoint to avoid errors.

PR 3382561: Virtual machines that share the same encryption key are randomly locked after the ESXi host reboots

When cloned from a single VM, several VMs can share the same encryption key. After an ESXi host reboot, each key of such VMs is added to the key cache, but while the first key addition succeeds, subsequent additions fail because the key already exists in the cache, and the key is removed. As a result, such VMs become locked.

This issue is resolved in this release.

ESXi-7.0U3v-24723872-no-tools

Profile Name	ESXi-7.0U3v-24723872-no-tools
Build	For build information, see the Patches Contained in This Release section.
Vendor	Broadcom, Inc.
Release Date	May 20, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_native-misc-drivers_7.0.3-0.145.24723872 • VMware_bootbank_vsan_7.0.3-0.145.24723872 • VMware_bootbank_bmcal_7.0.3-0.145.24723872 • VMware_bootbank_esx-xserver_7.0.3-0.145.24723872 • VMware_bootbank_gc_7.0.3-0.145.24723872 • VMware_bootbank_esx-base_7.0.3-0.145.24723872 • VMware_bootbank_esxio-combiner_7.0.3-0.145.24723872

	• VMware_bootbank_trx_7.0.3-0.145.24723872 • VMware_bootbank_cpu-microcode_7.0.3-0.145.24723872 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.145.24723872 • VMware_bootbank_vsanhealth_7.0.3-0.145.24723872 • VMware_bootbank_crx_7.0.3-0.145.24723872 • VMware_bootbank_vdfs_7.0.3-0.145.24723872 • VMware_bootbank_loadesx_7.0.3-0.145.24723872 • VMware_bootbank_esx-update_7.0.3-0.145.24723872 • VMW_bootbank_ntg3_4.1.15.0-4vmw.703.0.145.24723872 • VMW_bootbank_nvmetcp_1.0.0.7-1vmw.703.0.145.24723872
PRs Fixed	3406035, 3477734, 3489859, 3352051, 3457552, 3485174, 3469639, 3470731, 3485586, 3484794, 3484793, 3484786, 3477773, 3469106, 3477257, 3476746, 3475049, 3454755, 3469189, 3466996, 3458045, 3435833, 3447991, 3443815, 3432572, 3432690, 3441101, 3404668, 3434172, 3437311, 3371201, 3367834, 3398462, 3410295, 3390998, 3398458, 3388843, 3398467, 3430801, 3408807, 3420117, 3417327, 3423849, 3417227, 3417328, 3404126, 3408129, 3408008, 3408126, 3398534, 3400360, 3406033, 3398361, 3398279, 3407212, 3411695, 3396010, 3412537, 3352007, 3404202, 3402976, 3396464, 3407529, 3408143, 3336865, 3403867, 3389767, 3366075, 3365863, 3404507, 3403906, 3405760, 3401554, 3398537, 3355390, 3359530, 3393549, 3367426, 3359386, 3382561, 3358960, 3422040, 3412449, 3400844, 3365671, 3411044, 3437679, 3414590, 3364569
Related CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

This patch updates the following issues:

PR 3425364: Setting `cloud-init guestInfo` variables by regular users in the guest results into an error

Starting with ESXi 7.0 Update 3v, setting `cloud-init guestInfo` variables by regular users in the guest results into an error due to design changes.

This issue is resolved in this release. For more information, see KB 377267.

PR 3406033: ESXi host fails with a purple diagnostic screen due to a rare physical CPU (PCPU) lockup

In the vSphere Client, when you use the **Delete from Disk** option to remove a virtual machine from a vCenter system and delete all VM files from the datastore, including the configuration file and virtual disk files, if any of the files is corrupted, a rare issue with handling corrupted files in the delete path might lead to a PCPU lockup. As a result, the ESXi host fails with a purple diagnostic screen and a message such as `NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release.

PR 3484786: ESXi installation on an iSCSI LUN fails as the ESXi iSCSI Boot Firmware Table (iBFT) module fails to discover the LUN

In some cases, the iBFT control structure might have an optional expansion for which the ESXi vmkibft module doesn't have a proper check. As a result, iSCSI LUN discovery by using iBFT might fail and cause failure of the ESXi installation on the iSCSI LUN.

This issue is resolved in this release.

PR 3423217: You see vendor name of some Solidigm NVMe devices as Unknown

In the ESXi Host Client, under **Manage > Hardware > PCI Devices**, and in the vSphere Client, under **Host > Configure > Hardware > PCI Devices > All PCI Devices**, you might see the vendor name of some Solidigm NVMe devices as `Unknown`.

This issue is resolved in this release.

PR 3398537: ESXi host fails with a purple diagnostic screen due to an I/O race with an error PSOD @BlueScreen: ASSERT bora/lib/misc/bitvector.c:632

Due to a rare I/O race condition on virtual machines backed by a vSphere Virtual Volume, the ESXi host might fail with a purple diagnostic screen and an error such as `PSOD @BlueScreen: ASSERT bora/lib/misc/bitvector.c:632`.

This issue is resolved in this release.

PR 3371201: The hostd service might generate core dumps during upgrade from ESXi 6.7 to 7.x when SNMP traps are configured

In very rare cases, a missing SNMP port value when SNMP traps are configured during an upgrade from ESXi 6.7 to 7.x, might lead to hostd core dumps.

This issue is resolved in this release.

PR 3352051: Syslog configuration changes in a host profile that you use to provision ESXi host with Auto Deploy stateful install do not persist across reboots

If you change the syslog configuration of a host profile and provision ESXi hosts with that profile by using the Auto Deploy stateful install, changes might not persist after the hosts reboot.

This issue is resolved in this release.

PR 3396010: Controller VMs with direct I/O devices in third-party hyper converged infrastructure environments experience guest kernel soft lockups

A rare race condition between the interrupt virtualization and the VMkernel CPU scheduler in an ESXi host might result in guest kernel soft lockups on controller VMs with direct I/O devices in third-party hyper converged infrastructure environments. The soft locks cause virtual machines in the entire cluster to lose NFS storage connectivity and I/O access.

This issue is resolved in this release.

PR 3359386: If the Latency Sensitivity parameter of a virtual machine is set to High, you cannot add memory to that VM when powered off

If you use the vSphere Client to set the `Latency Sensitivity` parameter of a VM to `High`, attempts to add memory to such a VM when powered off might fail with an error such as `A specified parameter was not correct: spec.memoryAllocation`.

This issue is resolved in this release.

PR 3403867: Setting the CPU limit to 0 makes virtual machines unresponsive

If for any reason you set the CPU limit of running virtual machines to `0`, this causes CPU starvation and the VMs become unresponsive.

This issue is resolved in this release.

PR 3457552: You might see multiple hardware sensor alerts due to a Baseboard Management Controller (BMC) issue

An underlying BMC issue might cause ESXi hardware health monitoring to produce multiple alerts for hardware sensors on ESXi hosts, which you see in the vSphere Client under **Monitor > Tasks and Events**.

This issue is resolved in this release. The fix logs raw sensor data directly from IPMI to provide a data point to debug possible BMC issues that cause false alerts but cannot prevent BMC issues from occuring.

PR 3484794: Restoring the iSCSI configurations on an ESXi host might fail during boot due to stale entries in the ConfigStore database

If the ConfigStore database on an ESXi host has stale iSCSI configurations related to hardware iSCSI adapters, the iSCSI jumpstart might fail and restoring the iSCSI configuration on that host also fails during boot.

This issue is resolved in this release.

PR 3484793: Discovery of iSCSI dynamic targets, LUNs, and datastores fails on ESXi host reboot

In some cases, dynamic discovery of targets in systems that use dynamic discovery addresses for iSCSI configuration might fail. As a result, you do not see iSCSI targets, LUNs, and datastores after a reboot of ESXi hosts. The dynamic discovery of iSCSI targets might also fail when the Challenge-Handshake Authentication Protocol (CHAP) is active on the ESXi host.

This issue is resolved in this release.

PR 3458283: A rare Baseboard Management Controller (BMC) issue might cause some applications to become unresponsive

If an application sends an IPMI request to the BMC while it resets, such requests remain indefinitely pending and cause the applications to become unresponsive.

This issue is resolved in this release. The fix updates the IPMI driver to handle such conditions.

PR 3485174: Guest OS might mark file system read-only after repeated I/O failure which can cause Kubernetes control plane nodes to go into Read-only mode

An issue with the check for max allowed memory address in memory mapping code during I/O processing at virtual SCSI might cause a guest OS on an ESXi host to mark guest file system as read-only. As a result, Kubernetes control plane nodes might go into Read-only mode. In the vmkernel logs, you see multiple error messages such as `failed to pin: I/O error.`

This issue is resolved in this release.

PR 3470731: Unsupported SCSI Read Mode Sense Page commands to a Raw Disk Mapping (RDM) target might cause virtual machines to become unresponsive

A large number of unsupported SCSI Read Mode Sense Page commands to a RDM target from a VM configured with an RDM device might exceed the storage heap and cause both the datastore and the VM to become unresponsive.

This issue is resolved in this release. The fix prevents blocking VM I/O operations by optimizing the handling of unsupported SCSI commands or mode pages. Specifically, in passthrough mode used for RDM devices, the system no longer attempts to process such unsupported commands in a way that consumes storage heap resources.

PR 3398467: vSphere Virtual Volumes daemon fails after converting a VASA provider from external to internal

Due to an issue with handling IDs during an unbind operation for some vSphere API for Storage Awareness (VASA) providers, in some tasks such as converting a VASA provider from external to internal, the vSphere Virtual Volumes daemon vvold might fail as it cannot map unique IDs.

This issue is resolved in this release. With the fix, vvold gracefully handles such conditions and stops the unbind operation with message in the logs instead of failing.

PR 3414590: Snapshot tasks on virtual machines on NVMe/TCP datastores might take much longer than on VMs provisioned on NVMe/FC datastores

When creating or deleting a snapshot on a VM provisioned on datastores backed by NVMe/TCP namespaces, such tasks might take much longer than on VMs provisioned on datastores backed by NVMe/FC namespaces. The issue occurs because the nvmetcp driver handles some specific NVMe commands not in the way the NVMe/TCP target systems expect.

This issue is resolved in this release.

PR 3388843: You cannot activate Kernel DMA Protection on a virtual machine with Windows OS and Intel processor

When virtual Input-Output Memory Management Unit (vIOMMU) is active on a virtual machine with Windows OS and an Intel CPU, you might not be able to activate Kernel DMA Protection.

This issue is resolved in this release. The fix adds `acpi.dmar.enableDMAProtection=TRUE` to the vmx advanced settings that you can use if required.

PR 3469106: ESXi hosts intermittently disconnect from the Active Directory domain or from vCenter

Memory leaks might occur in Likewise during Active Directory operations or if smart card authentication is active on an ESXi host. As a result, Likewise processes might run out of memory and ESXi hosts intermittently disconnect from the Active Directory domain or from vCenter. In the `/var/log/vmkernel.log` file, you see messages similar to:

```
yyyy-mm-dd In(182) vmkernel: cpu72:2110465)uw.2110464 (44739) requires 1024 KB, asked 1024 KB from likewise (792) which has 93112 KB occupied and 72 KB available.
```

```
yyyy-mm-dd In(182) vmkernel: cpu72:2110465)Admission failure in path: host/vim/vmvisor/likewise:lwsmd.2110464:uw.2110464
```

In the `hostd-probe.log` file you see a message such as: `hostd detected to be non-responsive.`

This issue is resolved in this release. The fix adds a system service that monitors Likewise memory usage and restarts relevant services in case memory consumption approaches Likewise limits.

PR 3477734: ESXi host fails with a purple diagnostic screen while activating HClock

If for some reason an ESXi host fails to allocate memory for the activation of the HClock capability, the error handling goes into CPU wait state while it still holds a lock. As a result, the host fails with a purple diagnostic screen, and you see backtraces such as:

```
[0x2b8c]RCU_WaitForGracePeriod@vmkernel#nover stack:
[0xa000]vmk_HashRelease@vmkernel#nover+ stack:
[0xa0000]NetSchedHClkConnect@(netsched_hclk)#<None> stack:
```

This issue is resolved in this release.

PR 3489859: Migration of virtual machines fails with an error "Failed to allocate migration heap" on the source ESXi host

In very rare cases, if a virtual machine powers off before a running migration completes, ESXi might fail to clean up the migration heap. If the memory leak continues over time, the migration heap might be exhausted, and virtual machines cannot migrate from such ESXi hosts.

This issue is resolved in this release.

PR 3499302: If a virtual machine migrates to an ESXi host undergoing NSX update, the Distributed Firewall rule might be detached from that host

During NSX update or upgrade, ESXi hosts go into maintenance mode and the Distributed Resource Scheduler might trigger mass migration of VMs. As a result, vSphere vMotion with the Distributed Firewall rule might fail on some VMs and cause the DFW rule to be detached from the host.

This issue is resolved in this release.

PR 3477772: Encrypted virtual machines with active Change Block Tracking (CBT) might intermittently power off after a rekey operation

Due to a race condition between the VMX and hostd services for a specific VMcrypt-related reconfiguration, encrypted VMs with active CBT might unexpectedly power off during a rekey operation.

This issue is resolved in this release.

PR 3469639: Logging stops on all log files and configured remote host targets on ESXi hosts and hosts might become unresponsive

A rare deadlock situation in the ESXi log daemon vmsyslogd might cause logging to stop on all log files and configured remote host targets on ESXi hosts. As a result, the hosts might become unresponsive. The issue might occur as the result of multiple syslog reloads.

This issue is resolved in this release.

PR 3458045: ESXi hosts intermittently fail with purple diagnostic screen due to a rare race condition

A very rare race condition might lead to accessing an interface address while it is freed from another context. As a result, ESXi hosts might intermittently fail with purple diagnostic screen and an error such as `#PF Exception 14 in world 1001391810:dhclient-uw IP 0x420003562680`.

This issue is resolved in this release.

PR 3398458: ESXi hosts become unresponsive due to pointer blocks cached filling VMFS heap to its limit

Copies of pointer blocks that are part of data transactions between ESXi hosts might be cached in the VMFS heap even after the transactions are completed. Such cached pointer blocks might fill in the heap to its limit and as a result, ESXi hosts become unresponsive from vCenter and eventually virtual machines might go offline.

This issue is resolved in this release.

PR 3390998: ESXi hosts might fail with a purple diagnostic screen due to an incomplete cleanup of a SCSI path after deleting a controller

If a controller is deleted before a device claim process completes, the `namespace` object is removed, but the SCSI Path object remains. When adding a new `namespace`, the SCSI Path might prematurely become claimable, leading to a partially populated `PsaNvmePath` object. If a claim thread picks up that path before initialization, the ESXi host might fail with a purple diagnostic screen with an error such as:`@BlueScreen: #PF Exception 14 in world 1001448541:Cmpl-vmhba66 IP 0x420025354538 addr 0x0`.

This issue is resolved in this release.

PR 3358960: In the vmkernel logs, you see multiple errors from the network interface drivers for an unsupported feature

When the ESXi NetQueue load balancer, which uses load balancing algorithms to manage the vNIC and VMkernel adapter filters, sends a VMK_UPLINK_QUEUE_FEAT_LATENCY request to a nmlx5 driver, you see multiple errors in the vmkernel logs. VMK_UPLINK_QUEUE_FEAT_LATENCY is a software queue feature and if a client request contains this feature, the NIC drivers do not allocate queues but log errors that an unregistered feature is requested.

This issue is resolved in this release. The fix masks VMK_UPLINK_QUEUE_FEAT_LATENCY in requests for queue allocation from NIC drivers.

PR 3441399: You cannot upload virtual machine template of version ESXi 7.0 Update 3 with a DirectPath I/O device to the Content Library

When you create a template from an ESXi 7.0 Update 3 VM with a DirectPath I/O device, the upload to the Content Library fails with a `Null Pointer` exception. In the vSphere Client, you see an error such as `Failed to export OVF package. ThrowableProxy.cause A general runtime error occurred. An error occurred: java.lang.NullPointerException`. In the `cls.log`, you see the error `java.lang.NullPointerException: null`.

This issue is resolved in this release.

PR 3437679: ESXi host fails with a purple diagnostic screen due to mishandling a canceled NVMe write command

In rare cases, a large-size NVMe write command might be canceled due to an I/O timeout but the nvmetcp driver might again complete the command and this causes the ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3393549: Windows and Citrix virtual machines with vGPU intermittently fail with driver-related blue diagnostic screen

Windows and Citrix VMs with a vGPU device might intermittently run out of file handles and fail with a blue diagnostic screen.

This issue is resolved in this release. The fix allows you to increase the number of file handles to 16384 for Windows and Citrix VMs with a vGPU device. For more information, see KB 369633.

PR 3434172: You cannot apply a reverse path filter for virtual machines in promiscuous mode even though /Net/ReversePathFwdCheckPromisc is active

In very specific conditions, after an upgrade of a distributed virtual switch or uninstalling an NSX transport node on an ESXi host with converged distributed virtual switch that contains a port group with active promiscuous mode, you might see some networking issues, including:

1. You cannot apply a reverse path filter for virtual machines in promiscuous mode even though **/Net/ReversePathFwdCheckPromisc** is active.
2. Intermittent packet connectivity issues when using promiscuous mode on a distributed virtual switch with multiple uplinks.

This issue is resolved in this release.

PR 3420117: ESXi hosts become non-responding during a failover

In a failover task, ESXi sends the `INQUIRY page-83` command to the target host to get port parameters but in a ghost LUN configuration some target arrays might provide unformatted output for this command. As a result, the failover task fails and in the kernel logs you see the message `Target completed the Inquiry VPD Page 0x83 request with good status but returned junk data.`

This issue is resolved in this release.

PR 3437311: The intrusion detection and prevention system (IDS/IPS) might report false positives for dropped packets in vSphere reporting tools

In environments with active IDS/IPS, ESXi might report false positives for dropped packets to network monitoring solutions such as Aria Operations. If you deactivate IDS/IPS, the count of dropped packets falls. The issue affects all virtual machines connected to NSX segments.

This issue is resolved in this release.

PR 3398462: Virtual machines residing on a vSphere Virtual Volumes datastore might become inaccessible due to a size reporting issue

An issue in the VASA provider might report an inflated size for the home directory that contains metadata files for a virtual machine and VMFS automatically expands to accommodate the larger size. However, if the VASA provider later reports the correct size, VMFS cannot shrink, and the home directory cannot open. As a result, all VM files stored in the home folder become inaccessible and you cannot access the VMs.

This issue is resolved in this release.

PR 3411044: ESXi host might lose network connectivity due to a very rare issue with the ntg3 driver

A data race in the handling of tx queue full situation in the ntg3 driver might cause in very rare cases the TX queue to stop transmitting packets. As a result, you see either virtual machines or ESXi host management network, or both, lose connectivity. In the vmkernel log of the affected ESXi host, you see messages such as `Uplink: XXXX: Queue 0 of device vmnicX stuck, resetting the device` and/or `Vmxnet3: XXXXX: XXXX, portID(XXXXX): Hang detected.`

This issue is resolved in this release. The fix is part of ntg3 4.1.15.

PR 3407529: Virtual machines with snapshots and active encryption experience higher I/O latency

In rare cases, encrypted VMs with snapshots might experience higher than expected latency. This issue occurs due to unaligned I/O operations that generate excessive metadata requests to the underlying storage and lead to increased latency.

This issue is resolved in this release. To optimize performance, the VMcrypt I/O filter is enhanced to allocate memory in 4K-aligned blocks for both read and write operations. This reduction in metadata overhead significantly improves overall I/O performance.

PR 3410295: You see gaps in the collection of metrics for some virtual machines

Due to a time sync issue, collection of data for some VMs might fail and you do not see any performance data in platforms such as Aria Operations. In the */var/run/log/vobd.log* on the ESXi host, you see errors such as: `1149:2024-06-11T05:01:11.250Z: [ClockCorrelator] 7826272852729us: [vob.clock.correction.adjtime.sync] system clock synchronized to upstream time servers`

This issue is resolved in this release. The fix caches results from Stats Registry queries with selected dynamic counters to make sure metrics are consistent.

PR 3401554: vSAN Original Storage Architecture (OSA) virtual machines with large-sized VMDKs might experience performance degradation or become inaccessible

In vSAN OSA environments of version 8.0 and later, VMDK objects with a large amount of used capacity, such as close to the maximum of 62 TB, might overload the scrubber, which leads to a race condition that might cause such objects to experience performance degradation or become inaccessible.

This issue is resolved in this release.

PR 3359530: ESXi hosts fail with purple diagnostic screen due to a pNIC driver memory overload

In a rare situation when memory-intensive workloads that fragment system memory run in parallel with throughput-intensive workloads on a virtual switch configured with 9000 MTU or more, ESXi hosts might fail with a purple diagnostic screen. As a result, power-on virtual machines become temporarily unavailable. The issue occurs because memory allocation requests from the pNIC driver overload the memory subsystem with a growing networking packet heap, which causes ESXi to fail with a stack trace at `/var/cores/` such as:

```
NMI_Interrupt@vmkernel#nover+0x561
IDTNMIWork@vmkernel#nover+0x7f
Int2_NMI@vmkernel#nover+0x19
gate_entry@vmkernel#nover+0x68
Timer_GetCycles@vmkernel#nover+0x2
SP_WaitLockIRQ@vmkernel#nover+0xd5
SPLockIRQWork@vmkernel#nover+0x3e
Heap_AlignWithTimeoutAndRA@vmkernel#nover+0xea
Pkt_AllocHandleWithSize@vmkernel#nover+0x165
Pkt_AllocWithFlags@vmkernel#nover+0xd
vmk_PktAllocForDMAEngine@vmkernel#nover+0x46
```

This issue is resolved in this release. With the fix, you can reserve enough memory for the pNIC driver using the command `esxcli system settings kernel set -s netPktJumboSlabMinSize -v <MEMORY_SIZE_TO_RESERVE_IN_MB>` . To define the amount of memory you need to reserve, use this formula: `reservation size = (numPnics * numRxQueues * (rxRingSize + 64) + numPcpus *256) * 10KB`. For example, for an ESXi host with 72 PCPUs and 4 PNICs with 10 queues of ring size set to 4K each, the reservation is about 2048 MB.

PR 3412449: Remediation of ESXi hosts might fail due to a timeout in the update of the VMware-VM-Tools component

While upgrading ESXi hosts by using vSphere Lifecycle Manager, remediation of the VMware-VM-Tools component might occasionally fail due to a timeout. The issue occurs when the update process takes longer than the timeout setting of 30 sec for the VMware-VM-Tools component.

This issue is resolved in this release. The fix increases the timeout limit to 120 sec.

PR 3400360: VMFS6 automatic UNMAP feature might fail to reclaim filesystem space beyond 250GB

In certain cases, when you delete a filesystem space of more than 250GB on a VMFS6 volume, for example 1 TB, if the volume has no active references such as active VMs, then the VMFS6 automatic UNMAP feature might fail to reclaim the filesystem space beyond 250GB.

This issue is resolved in this release.

PR 3355390: An ESXi host fails with a purple diagnostic screen and message @BlueScreen: NMI IPI: Panic requested by another PCPU

If firewall rules in your environment result in packets moving across multiple portsets, a race condition might cause software locks to end in a deadlock. As a result, an ESXi host might fail with a purple diagnostic screen and message `@BlueScreen: NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release.

PR 3404507: ESXi hosts might fail with purple diagnostic screen due to a rare memory allocation error

If a VM power-on fails, a function that allocates memory on the heap might not free certain allocations and cause a memory leak. As a result, the ESXi host fails with a purple diagnostic screen in `World_DestroyHeap` with `NOT_IMPLEMENTED bora/vmkernel/main/world.c:2293` and `Unable to complete wait for non-empty heap` errors.

This issue is resolved in this release. The fix makes sure a cleanup function runs to free allocations to prevent the issue.

PR 3406156: Extracting a vSphere Lifecycle Manager image from an existing ESXi host might fail after a kernel configuration change

Each update of the kernel configuration also triggers an update to the `/bootbank/useropts.gz` file, but due to a rare issue, the `basemisc.tgz` might not contain the default `useropts` file after such an update. As a result, when attempting to extract a vSphere Lifecycle Manager image from an existing ESXi host, the absence of the default `useropts` file leads to failure to create the `esx-base.vib` file and the operational also fails.

This issue is resolved in this release.

PR 3396464: A lost cleanup callback might cause purple diagnostic screen failures in vSAN clusters with Remote Direct Memory Access (RDMA)

In Express Storage Architecture (ESA) vSAN clusters with active RDMA, a rare issue with a lost cleanup callback might cause a purple diagnostic screen failure with a message such as `Failed to wait for object exit.` The issue is specific to RDMA use in vSAN.

This issue is resolved in this release.

PR 3398279: Creating a vSAN File Service fails when you use IPs within the 172.17.0.0/16 range as mount points

Prior to vSphere 7.0 Update 3v, you must change your network configuration in cases when the specified file service network overlaps with the Docker default internal network 172.17.0.0/16. As a result, in the network configuration step of the File Service activation workflow, when you enter a subnet with 172.17.**.**, you see a warning and you cannot create vSAN File Services.

This issue is resolved in this release. The fix routes traffic to the correct endpoint to avoid possible conflicts. The fix is in the vSAN File Service Virtual Machine, and if you upgrade the file service to 7.0 Update 3v, you can ignore the conflict warning and continue the file service activation with subnet 172.17.0.0/16.

PR 3365863: ESXi hosts might fail with a purple diagnostic screen during high volume of outstanding I/O requests combined with slow storage performance

Under heavy I/O loads, a bug in the ESXi storage stack can cause an ESXi host to fail with a purple diagnostics screen if the storage cannot process the I/O requests quickly and some virtual machines on the ESXi host start issuing I/O resets.

This issue is resolved in this release.

PR 3364569: If a NVMe/TCP driver fails to process an I/O command, an ESXi host might disconnect from a storage array

If your ESXi hosts connect to storage arrays and perform read/write operations by using NVMe/TCP connections, when a NVMe/TCP driver fails to process an I/O command, ESXi might cancel the process with an abort command. As a result, an ESXi host might disconnect from a storage array and end previous I/O queues.

This issue is resolved in this release.

PR 3332717: An ESXi hosts might fail with a purple diagnostic screen during a file close on a NFS41 datastore

A file close on a NFS41 datastore might lead to memory corruption in a layer common across file systems. A subsequent file open on an NFSv3 datastore picks up the same memory zone. As a result, the ESXi host might fail with a purple diagnostic screen with a backtrace similar to:

```
NFSDestroySchedQueue NFS
Sched_DestroySchedQueue
NFSVolume_DestroySchedQHandle
```

This issue is resolved in this release.

PR 3352007: ESXi hosts might fail with a purple diagnostics screen and with errors for CpuSchedWait() and FS3_ReportCorruption() in the backtrace

In a data corruption scenario, the corruption report routine requires to load the VMFS datastore volume header metadata and perform a validation. In very rare cases, a spinlock might prevent reading this metadata and as a result, ESXi hosts might fail with a purple diagnostics screen. In the backtrace, you see errors for `CpuSchedWait()` and `FS3_ReportCorruption()`.

This issue is resolved in this release. The fix enhances the data corruption report routine to allow skipping the read on the volume header metadata for such rare cases.

PR 3367834: A fault tolerance secondary virtual machine might restart by accident

In very rare cases, a fault tolerance secondary VM might restart unexpectedly while other fault tolerance VMs power off or migrate from the ESXi host.

This issue is resolved in this release.

PR 3389767: During a vSphere vMotion migration of a fault tolerant Primary VM with encryption, the migration task might fail and vSphere FT failover occurs

In rare cases, the encryption key package might not be sent or received correctly during a vSphere vMotion migration of a fault tolerant Primary VM with encryption, and as a result the migration task fails and vSphere FT failover occurs.

This issue is resolved in this release. The fix sends the encryption key at the end of the vSphere FT checkpoint to avoid errors.

PR 3382561: Virtual machines that share the same encryption key are randomly locked after the ESXi host reboots

When cloned from a single VM, several VMs can share the same encryption key. After an ESXi host reboot, each key of such VMs is added to the key cache, but while the first key addition succeeds, subsequent additions fail because the key already exists in the cache, and the key is removed. As a result, such VMs become locked.

This issue is resolved in this release.

ESXi-7.0U3sv-24723868-standard

Profile Name	ESXi-7.0U3sv-24723868-standard
Build	For build information, see the Patches Contained in This Release section.
Vendor	Broadcom, Inc.
Release Date	May 20, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_bmcal_7.0.3-0.140.24723868 • VMware_bootbank_trx_7.0.3-0.140.24723868 • VMware_bootbank_esxio-combiner_7.0.3-0.140.24723868 • VMware_bootbank_esx-xserver_7.0.3-0.140.24723868 • VMware_bootbank_vsan_7.0.3-0.140.24723868 • VMware_bootbank_native-misc-drivers_7.0.3-0.140.24723868 • VMware_bootbank_gc_7.0.3-0.140.24723868 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.140.24723868 • VMware_bootbank_vdfs_7.0.3-0.140.24723868 • VMware_bootbank_crx_7.0.3-0.140.24723868 • VMware_bootbank_vsanhealth_7.0.3-0.140.24723868 • VMware_bootbank_cpu-microcode_7.0.3-0.140.24723868 • VMware_bootbank_esx-base_7.0.3-0.140.24723868 • VMware_bootbank_esx-update_7.0.3-0.140.24723868 • VMware_bootbank_loadesx_7.0.3-0.140.24723868 • VMware_locker_tools-light_12.5.1.24649672-24723868
PRs Fixed	3452679, 3488111, 3456430, 3450561, 3482267, 3479599, 3484230, 3476566, 3452717, 3432584, 3475105, 3470206, 3452699, 3435458, 3404661, 3400981, 3444626, 3469216, 3454671, 3469563, 3457662, 3447985, 3443017, 3432572, 3432690, 3404668, 3430751, 3400984, 3406922, 3430750, 3406923, 3425364, 3398141, 3406188, 3400967, 3430766, 3316536, 3408358, 3408125, 3390665, 3411970, 3412457, 3400130, 3404669, 3386280, 3494213, 3409318
Related CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

This patch updates the following issues:

ESXi 7.0 Update 3v includes the following Intel microcode:

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	baseline	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	baseline	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Arrandale	0x20655 (06/25/5)	0x92	baseline	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	baseline	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	baseline	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	baseline	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	baseline	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	baseline	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	baseline	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	baseline	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Haswell DT	0x306c3 (06/3c/3)	0x32	baseline	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	baseline	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	baseline	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	baseline	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	baseline	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	baseline	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	baseline	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	baseline	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Skylake SP	0x50654 (06/55/4)	0xb7	baseline	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	baseline	0x4003801	8/1/2024	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	baseline	0x5003801	8/1/2024	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	baseline	0x7002a01	8/1/2024	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	baseline	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	baseline	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	baseline	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	baseline	0xe000015	8/3/2023	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	baseline	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	baseline	0x3e	10/5/2023	Intel Atom C3000 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Ice Lake SP	0x606a6 (06/6a/6)	0x87	baseline	0xd0003f5	8/2/2024	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	baseline	0x10002c0	8/8/2024	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	baseline	0x4c000026	2/28/2024	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	baseline	0x4c000026	2/28/2024	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	baseline	0xba	8/1/2024	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	baseline	0x3a	8/1/2024	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	baseline	0x54	8/1/2024	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	baseline	0x2c0003e0	7/30/2024	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	baseline	0x2b000620	7/30/2024	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	baseline	0xf8	9/28/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/ a)	0x22	baseline	0xfa	7/28/2024	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/ b)	0x02	baseline	0xf6	2/1/2024	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	baseline	0xf8	2/1/2024	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/ d)	0x22	baseline	0x102	7/31/2024	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/ a7/1)	0x02	baseline	0x63	8/1/2024	Intel Xeon E-2300 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Raptor Lake E/HX/S	0xb0671 (06/b7/1)	0x32	baseline	0x12c	9/25/2024	Intel Xeon E-2400 Series
Emerald Rapids SP	0xc06f2 (06/cf/2)	0x87	baseline	0x21000291	7/30/2024	Intel Xeon 8500 Series; Intel Xeon Gold 6500/5500 Series; Intel Xeon Silver 4500 Series; Intel Xeon Bronze 3500 Series

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3v:

- **windows.iso**: VMware Tools 12.5.1 supports the following 64-bit Windows versions:- Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  For **windows.iso** support for 32-bit Windows versions: Windows 7 SP1 or Windows Server 2008 R2 SP1 and later, refer to VMware Tools 12.4.5 Release Notes.
  VMware Tools 12.5.0 provides support for Windows Server 2025, but make sure your system supports Windows 2025 if you plan to use Windows 2025 as a guest OS on virtual machines. For more information, see Installing Windows Server 2025 on a VMware Virtual Machine.
- **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. For more details, see VMware knowledge base article 88698.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- Updating VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- What Every vSphere Admin Must Know About VMware Tools
- Earlier versions of VMware Tools
- VMware Tools 12.5.1 Release Notes

PR 3408358: Security scans on ESXi hosts with OpenSSH 8.8 show multiple CVEs

When for some reason you need to activate OpenSSH on an ESXi host, if the OpenSSH version is 8.8 and you run a security scan, you might see multiple CVEs.

This issue is resolved in this release. The fix updates OpenSSH to version 9.3p2 and backports security fixes from later versions: CVE-2024-6387, CVE-2023-51385, CVE-2023-51384, CVE-2023-48795, CVE-2023-38408. The version string is updated to **OpenSSH_9.3p2 vmw9.8p1** to indicate the backported patches.

ESXi-7.0U3sv-24723868-no-tools

Profile Name	ESXi-7.0U3sv-24723868-no-tools
Build	For build information, see the Patches Contained in This Release section.
Vendor	Broadcom, Inc.
Release Date	May 20, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_bmcal_7.0.3-0.140.24723868 • VMware_bootbank_trx_7.0.3-0.140.24723868 • VMware_bootbank_esxio-combiner_7.0.3-0.140.24723868 • VMware_bootbank_esx-xserver_7.0.3-0.140.24723868 • VMware_bootbank_vsan_7.0.3-0.140.24723868 • VMware_bootbank_native-misc-drivers_7.0.3-0.140.24723868 • VMware_bootbank_gc_7.0.3-0.140.24723868 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.140.24723868 • VMware_bootbank_vdfs_7.0.3-0.140.24723868 • VMware_bootbank_crx_7.0.3-0.140.24723868 • VMware_bootbank_vsanhealth_7.0.3-0.140.24723868 • VMware_bootbank_cpu-microcode_7.0.3-0.140.24723868 • VMware_bootbank_esx-base_7.0.3-0.140.24723868 • VMware_bootbank_esx-update_7.0.3-0.140.24723868 • VMware_bootbank_loadesx_7.0.3-0.140.24723868
PRs Fixed	3452679, 3488111, 3456430, 3450561, 3482267, 3479599, 3484230, 3476566, 3452717, 3432584, 3475105, 3470206, 3452699, 3435458, 3404661, 3400981, 3444626, 3469216, 3454671, 3469563, 3457662, 3447985, 3443017, 3432572, 3432690, 3404668, 3430751, 3400984, 3406922, 3430750, 3406923, 3425364, 3398141, 3406188, 3400967, 3430766, 3316536, 3408358, 3408125, 3390665, 3411970, 3412457, 3400130, 3404669, 3386280, 3494213, 3409318
Related CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

This patch updates the following issues:

ESXi 7.0 Update 3v includes the following Intel microcode:

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	baseline	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	baseline	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Arrandale	0x20655 (06/25/5)	0x92	baseline	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	baseline	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	baseline	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	baseline	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	baseline	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	baseline	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	baseline	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	baseline	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Haswell DT	0x306c3 (06/3c/3)	0x32	baseline	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	baseline	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	baseline	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	baseline	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	baseline	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	baseline	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	baseline	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	baseline	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Skylake SP	0x50654 (06/55/4)	0xb7	baseline	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	baseline	0x4003801	8/1/2024	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	baseline	0x5003801	8/1/2024	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	baseline	0x7002a01	8/1/2024	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	baseline	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	baseline	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	baseline	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	baseline	0xe000015	8/3/2023	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	baseline	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	baseline	0x3e	10/5/2023	Intel Atom C3000 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Ice Lake SP	0x606a6 (06/6a/6)	0x87	baseline	0xd0003f5	8/2/2024	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	baseline	0x10002c0	8/8/2024	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	baseline	0x4c000026	2/28/2024	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	baseline	0x4c000026	2/28/2024	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	baseline	0xba	8/1/2024	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	baseline	0x3a	8/1/2024	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	baseline	0x54	8/1/2024	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	baseline	0x2c0003e0	7/30/2024	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	baseline	0x2b000620	7/30/2024	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	baseline	0xf8	9/28/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/ a)	0x22	baseline	0xfa	7/28/2024	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/ b)	0x02	baseline	0xf6	2/1/2024	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	baseline	0xf8	2/1/2024	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/ d)	0x22	baseline	0x102	7/31/2024	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/ a7/1)	0x02	baseline	0x63	8/1/2024	Intel Xeon E-2300 Series

Code Name	FMS	Plat ID	Servicing	MCU Rev	MCU Date	Brand Names
Raptor Lake E/HX/S	0xb0671 (06/b7/1)	0x32	baseline	0x12c	9/25/2024	Intel Xeon E-2400 Series
Emerald Rapids SP	0xc06f2 (06/cf/2)	0x87	baseline	0x21000291	7/30/2024	Intel Xeon 8500 Series; Intel Xeon Gold 6500/5500 Series; Intel Xeon Silver 4500 Series; Intel Xeon Bronze 3500 Series

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3v:

- **windows.iso**: VMware Tools 12.5.1 supports the following 64-bit Windows versions:- Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  For **windows.iso** support for 32-bit Windows versions: Windows 7 SP1 or Windows Server 2008 R2 SP1 and later, refer to VMware Tools 12.4.5 Release Notes.
  VMware Tools 12.5.0 provides support for Windows Server 2025, but make sure your system supports Windows 2025 if you plan to use Windows 2025 as a guest OS on virtual machines. For more information, see Installing Windows Server 2025 on a VMware Virtual Machine.
- **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. For more details, see VMware knowledge base article 88698.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- Updating VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- What Every vSphere Admin Must Know About VMware Tools
- Earlier versions of VMware Tools
- VMware Tools 12.5.1 Release Notes

PR 3408358: Security scans on ESXi hosts with OpenSSH 8.8 show multiple CVEs

When for some reason you need to activate OpenSSH on an ESXi host, if the OpenSSH version is 8.8 and you run a security scan, you might see multiple CVEs.

This issue is resolved in this release. The fix updates OpenSSH to version 9.3p2 and backports security fixes from later versions: CVE-2024-6387, CVE-2023-51385, CVE-2023-51384, CVE-2023-48795, CVE-2023-38408. The version string is updated to **OpenSSH_9.3p2 vmw9.8p1** to indicate the backported patches.

ESXi 7.0 U3v - 24723872

Name	ESXi
Version	ESXi 7.0 U3v - 24723872
Release Date	May 20, 2025
Category	BugFix
Affected Components	• ESXi Component - core ESXi • ESXi Install/Upgrade • ESXi Tools Component
PRs Fixed	3406035, 3477734, 3489859, 3352051, 3457552, 3485174, 3469639, 3470731, 3485586, 3484794, 3484793, 3484786, 3477773, 3469106, 3477257, 3476746, 3475049, 3454755, 3469189, 3466996, 3458045, 3435833, 3447991, 3443815, 3432572, 3432690, 3441101, 3404668, 3434172, 3437311, 3371201, 3367834, 3398462, 3410295, 3390998, 3398458, 3388843, 3398467, 3430801, 3408807, 3420117, 3417327, 3423849, 3417227, 3417328, 3404126, 3408129, 3408008, 3408126, 3398534, 3400360, 3406033, 3398361, 3398279, 3407212, 3411695, 3396010, 3412537, 3352007, 3404202, 3402976, 3396464, 3407529, 3408143, 3336865, 3403867, 3389767, 3366075, 3365863, 3404507, 3403906, 3405760, 3401554, 3398537, 3355390, 3359530, 3393549, 3367426, 3359386, 3382561, 3358960, 3422040, 3412449, 3400844, 3365671, 3411044, 3437679, 3414590, 3364569
Related CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

This patch resolves the issues listed in the ESXi-7.0U3v-24723872-standard image profile.

ESXi 7.0 U3sv - 24723868

Name	ESXi
Version	ESXi 7.0 U3sv - 24723868
Release Date	May 20, 2025
Category	Security
Affected Components	• ESXi Component - core ESXi • ESXi Install/Upgrade • ESXi Tools Component
PRs Fixed	3452679, 3488111, 3456430, 3450561, 3482267, 3479599, 3484230, 3476566, 3452717, 3432584, 3475105, 3470206, 3452699, 3435458, 3404661, 3400981, 3444626, 3469216, 3454671, 3469563, 3457662, 3447985, 3443017, 3432572, 3432690, 3404668, 3430751, 3400984, 3406922, 3430750, 3406923, 3425364, 3398141, 3406188, 3400967, 3430766, 3316536, 3408358, 3408125, 3390665, 3411970, 3412457, 3400130, 3404669, 3386280, 3494213, 3409318
Related CVE numbers	CVE-2025-41226, CVE-2025-41227, CVE-2025-41228

This patch resolves the issues listed in the ESXi-7.0U3sv-24723868-standard image profile.

Known Issues

vSAN Issues

When rebooting a vSAN host, other hosts in the vSAN cluster enter a partitioned state

During ESXi shutdown, hosts in a vSAN cluster can enter a state where they can transmit but not receive data. Depending of the exact timing and duration of this state, this state can lead to unexpected role changes in the vSAN distributed cluster membership, monitoring, and directory service (CMMDS). Consequently, vSAN hosts might continually attempt to reform a cluster with the rebooting host or send CMMDS updates through the rebooting host, which is unresponsive to incoming traffic. As a result, in the vSAN Health monitoring you see `vSAN Cluster Partition` alarms.

Workaround: Before rebooting a vSAN host, identify all vmknics on the host with tags `VSAN` , `VSANWitness` , or `VSANExternal` , take note of which vSAN tag is used on each vmknic, and remove the tags. After rebooting, reapply the tags for vSAN traffic by type and vmknic.

Known Issues from Previous Releases

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Corrupted VFAT partitions from a vSphere 6.7 environment might cause upgrades to ESXi 7.x to fail

Due to corrupted VFAT partitions from a vSphere 6.7 environment, repartitioning the boot disks of an ESXi host might fail during an upgrade to ESXi 7.x. As a result, you might see the following errors:

When upgrading to ESXi 7.0 Update 3l, the operation fails with a purple diagnostic screen and/or an error such as:

- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to calculate size for temporary Ramdisk: <error>.`
- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to copy files to Ramdisk: <error>.`
  If you use an ISO installer, you see the errors, but no purple diagnostic screen.

When upgrading to an ESXi 7.x version earlier than 7.0 Update 3l, you might see:

- Logs such as `ramdisk (root) is full` in the `vmkwarning.log` file.
- Unexpected rollback to ESXi 6.5 or 6.7 on reboot.
- The `/bootbank` ,`/altbootbank` , and ESX-OSData partitions are not present.

Workaround: You must first remediate the corrupted partitions before completing the upgrade to ESXi 7.x. For more details, see VMware knowledge base article 91136.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the
requirement cannot be satisfied within the ImageProfile. Please refer to the log file for
more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
```

```
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
 The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
 Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s).`

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU.`

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer.`

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network.` This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Set-VMHostService -policy "off"$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx`, the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1`.

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set --tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer": { "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"`, run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command:
   `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command:
   `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command:
   `esxcli network firewall load.`
5. Start the hostd service by using the command:
   `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats`, you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835`.

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0`.

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For

example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set` **-o** `/USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.
2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

vSAN Issues

PR 2962316: vSAN File Service does not support NFSv4 delegations

vSAN File Service does not support NFSv4 delegations in this release.

Workaround: None

PR 3235496: Applications on a vSAN cluster become intermittently unresponsive

If the advanced option `preferHT` is enabled on an AMD server in a vSAN cluster, the virtual CPUs of a virtual machine run on the same last level cache. When the virtual CPUs are all very busy and an NVMe thread to handle I/Os happens to run also on the same last level cache, the NVMe thread takes very long to complete, because it competes for CPU resources with the busy VMs. As a result, the I/O latency is very high and might lead to intermittent unresponsiveness of storage and applications on the vSAN cluster. In the backlog, you see errors such as `Lost access to volume <uuid> due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.`

Workaround: Use the command `esxcli system settings advanced set -o /Misc/vmknvmeCwYield -I 0` to avoid competition between the NVMe completion queue and busy virtual CPUs.

VMware ESXi 7.0 Update 3s Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Patch Download and Installation

- Resolved Issues
- Known Issues from Previous Releases

Introduction

VMware ESXi 7.0 Update 3s |04 MAR 2025 | Build 24585291 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3s, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3s. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- This release resolves CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0004.

Patches Contained in This Release

This release of ESXi 7.0 Update 3s delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3s-24585291-depot.zip
Build:	24585291
Download Size:	382.1 MB
md5sum:	6535f6f9a016fb1a76d6caa086f48891
sha256checksum:	b4de8b0b2b0bf9851dcef9f30cb19ff487b03d8494693acec216eb9635f4dd59
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.135.24585291	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.135.24585291	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include

all of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:

- VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
- VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
- VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
- VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3s-24585291	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3s-24585291-standard
ESXi-7.0U3s-24585291-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi7.0U3s - 24585291	March 04 2025	Security	Security only image

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.135.24585291

Patch Category	Security

Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_vdfs_7.0.3-0.135.24585291 • VMware_bootbank_cpu-microcode_7.0.3-0.135.24585291 • VMware_bootbank_crx_7.0.3-0.135.24585291 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.135.24585291 • VMware_bootbank_esx-xserver_7.0.3-0.135.24585291 • VMware_bootbank_gc_7.0.3-0.135.24585291 • VMware_bootbank_native-misc-drivers_7.0.3-0.135.24585291 • VMware_bootbank_trx_7.0.3-0.135.24585291 • VMware_bootbank_vsan_7.0.3-0.135.24585291 • VMware_bootbank_esxio-combiner_7.0.3-0.135.24585291 • VMware_bootbank_bmcal_7.0.3-0.135.24585291 • VMware_bootbank_esx-base_7.0.3-0.135.24585291 • VMware_bootbank_vsanhealth_7.0.3-0.135.24585291
PRs Fixed	N/A
CVE numbers	CVE-2025-22224, CVE-2025-22225, CVE-2025-22226

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

This patch updates the `esx-base` VIB. Due to their dependency with the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `vdfs`, `cpu-microcode`, `crx`, `esx-dvfilter-generic-fastpath`, `esx-xserver`, `gc`, `native-misc-drivers`, `trx`, `vsan`, `esxio-combiner`, `bmcal`, `vsanhealth` , and `esx-base` . This patch resolves the following issue:

This release resolves CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0004.

esx-update_7.0.3-0.135.24585291

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.135.24585291 • VMware_bootbank_esx-update_7.0.3-0.135.24585291
PRs Fixed	N/A
CVE numbers	N/A

Due to their dependency on the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `loadesx` and `esx-update` .

ESXi-7.0U3s-24585291-standard

Profile Name	ESXi-7.0U3s-24585291-standard
Build	For build information, see Patches Contained in This Release.
Vendor	Broadcom
Release Date	March 04, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vdfs_7.0.3-0.135.24585291 • VMware_bootbank_cpu-microcode_7.0.3-0.135.24585291 • VMware_bootbank_crx_7.0.3-0.135.24585291 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.135.24585291 • VMware_bootbank_esx-xserver_7.0.3-0.135.24585291 • VMware_bootbank_gc_7.0.3-0.135.24585291 • VMware_bootbank_native-misc-drivers_7.0.3-0.135.24585291 • VMware_bootbank_trx_7.0.3-0.135.24585291 • VMware_bootbank_vsan_7.0.3-0.135.24585291 • VMware_bootbank_esxio-combiner_7.0.3-0.135.24585291 • VMware_bootbank_bmcal_7.0.3-0.135.24585291 • VMware_bootbank_esx-base_7.0.3-0.135.24585291 • VMware_bootbank_vsanhealth_7.0.3-0.135.24585291 • VMware_bootbank_loadesx_7.0.3-0.135.24585291 • VMware_bootbank_esx-update_7.0.3-0.135.24585291
PRs Fixed	N/A
Related CVE numbers	CVE-2025-22224, CVE-2025-22225, CVE-2025-22226

This patch updates the following issue:

This release resolves CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0004.

ESXi-7.0U3s-24585291-no-tools

Profile Name	ESXi-7.0U3s-24585291-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	Broadcom
Release Date	March 04, 2025
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vdfs_7.0.3-0.135.24585291

	• VMware_bootbank_cpu-microcode_7.0.3-0.135.24585291 • VMware_bootbank_crx_7.0.3-0.135.24585291 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.135.24585291 • VMware_bootbank_esx-xserver_7.0.3-0.135.24585291 • VMware_bootbank_gc_7.0.3-0.135.24585291 • VMware_bootbank_native-misc-drivers_7.0.3-0.135.24585291 • VMware_bootbank_trx_7.0.3-0.135.24585291 • VMware_bootbank_vsan_7.0.3-0.135.24585291 • VMware_bootbank_esxio-combiner_7.0.3-0.135.24585291 • VMware_bootbank_bmcal_7.0.3-0.135.24585291 • VMware_bootbank_esx-base_7.0.3-0.135.24585291 • VMware_bootbank_vsanhealth_7.0.3-0.135.24585291 • VMware_bootbank_loadesx_7.0.3-0.135.24585291 • VMware_bootbank_esx-update_7.0.3-0.135.24585291
PRs Fixed	N/A
Related CVE numbers	CVE-2025-22224, CVE-2025-22225, CVE-2025-22226

This patch updates the following issue:

This release resolves CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226. For more information on these vulnerabilities and their impact on Broadcom products, see VMSA-2025-0004.

ESXi7.0U3s - 24585291

Name	ESXi
Version	ESXi7.0U3s - 24585291
Release Date	March 04, 2025
Category	Security
Affected Components	• ESXi Component - core ESXi • ESXi Install/Upgrade
PRs Fixed	N/A
Related CVE numbers	CVE-2025-22224, CVE-2025-22225, CVE-2025-22226

This patch resolves the issues listed in ESXi_7.0.3-0.135.24585291.

Known Issues from Previous Releases

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Corrupted VFAT partitions from a vSphere 6.7 environment might cause upgrades to ESXi 7.x to fail

Due to corrupted VFAT partitions from a vSphere 6.7 environment, repartitioning the boot disks of an ESXi host might fail during an upgrade to ESXi 7.x. As a result, you might see the following errors:

When upgrading to ESXi 7.0 Update 3l, the operation fails with a purple diagnostic screen and/or an error such as:

- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to calculate size for temporary Ramdisk: <error>.`
- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to copy files to Ramdisk: <error>.`
  If you use an ISO installer, you see the errors, but no purple diagnostic screen.

When upgrading to an ESXi 7.x version earlier than 7.0 Update 3l, you might see:

- Logs such as `ramdisk (root) is full` in the `vmkwarning.log` file.
- Unexpected rollback to ESXi 6.5 or 6.7 on reboot.
- The `/bootbank`,`/altbootbank`, and ESX-OSData partitions are not present.

Workaround: You must first remediate the corrupted partitions before completing the upgrade to ESXi 7.x. For more details, see VMware knowledge base article 91136.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the requirement cannot be satisfied within the ImageProfile. Please refer to the log file for more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
 The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
 Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s)`.

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU`.

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer.`

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq “slpd”} | Set-VMHostService -policy “off”$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq “slpd”} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx` , the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1`.

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set --tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer": { "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"`, run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo`"

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo`"

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first

disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command: `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command: `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command: `esxcli network firewall load.`
5. Start the hostd service by using the command: `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats`, you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835`.

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0`.

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set -o /USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.

2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

vSAN Issues

PR 2962316: vSAN File Service does not support NFSv4 delegations

vSAN File Service does not support NFSv4 delegations in this release.

Workaround: None

PR 3235496: Applications on a vSAN cluster become intermittently unresponsive

If the advanced option `preferHT` is enabled on an AMD server in a vSAN cluster, the virtual CPUs of a virtual machine run on the same last level cache. When the virtual CPUs are all very busy and an NVMe thread to handle I/Os happens to run also on the same last level cache, the NVMe thread takes very long to complete, because it competes for CPU resources with the busy VMs. As a result, the I/O latency is very high and might lead to intermittent unresponsiveness of storage and applications on the vSAN cluster. In the backlog, you see errors such as `Lost access to volume <uuid> due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.`

Workaround: Use the command `esxcli system settings advanced set -o /Misc/vmknvmeCwYield -I 0` to avoid competition between the NVMe completion queue and busy virtual CPUs.

VMware ESXi 7.0 Update 3r Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues from Previous Releases

Introduction

VMware ESXi 7.0 Update 3r | 12 DEC 2024 | Build 24411414 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3r, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3r. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

This release resolves an issue with vSphere vMotion tasks that fail with an error `NamespaceMgr could not lock the db file.`

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3q Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3p Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3o Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3n Release Notes

- VMware ESXi 7.0, ESXi 7.0 Update 3m Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3l Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Patches Contained in This Release

This release of ESXi 7.0 Update 3r delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3r-24411414-depot.zip
Build:	24411414
Download Size:	382.0 MB
md5sum:	03433d753ef408ce939dd3a59fd80594
sha256checksum:	82724ee9d297a7cecb0f473c27b44b7401e227db99ea0046e15a2cd7a115ade7
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.130.24411414	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.130.24411414	Bugfix	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3r-24411414	Bugfix	Critical	Bugfix only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3r-24411414-standard
ESXi-7.0U3r-24411414-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi7.0U3r - 24411414	DEC 12 2024	Bugfix	Bugfix only image

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.130.24411414

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_bmcal_7.0.3-0.130.24411414 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.130.24411414 • VMware_bootbank_vdfs_7.0.3-0.130.24411414 • VMware_bootbank_cpu-microcode_7.0.3-0.130.24411414 • VMware_bootbank_gc_7.0.3-0.130.24411414 • VMware_bootbank_vsanhealth_7.0.3-0.130.24411414 • VMware_bootbank_trx_7.0.3-0.130.24411414 • VMware_bootbank_crx_7.0.3-0.130.24411414 • VMware_bootbank_esx-xserver_7.0.3-0.130.24411414 • VMware_bootbank_vsan_7.0.3-0.130.24411414 • VMware_bootbank_native-misc-drivers_7.0.3-0.130.24411414 • VMware_bootbank_esxio-combiner_7.0.3-0.130.24411414 • VMware_bootbank_esx-base_7.0.3-0.130.24411414
PRs Fixed	3459675
CVE numbers	N/A

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

This patch updates the `esx-base` VIB. Due to their dependency with the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `bmcal`, `esx-dvfilter-generic-fastpath`, `vdfs`, `cpu-microcode`, `gc`, `vsanhealth`, `trx`, `crx`, `esx-xserver`, `vsan`, `native-misc-drivers`, `esxio-combiner` , and `esx-base` . This patch resolves the following issue:

vSphere vMotion tasks fail with an error NamespaceMgr could not lock the db file

In rare cases, when virtual machines are configured with namespaces, an issue with the namespace database might cause migration of such VMs with vSphere vMotion to fail. In the vSphere Client, you see errors such as:

```
Failed to receive migration. The source detected that the destination failed to resume.
```

```
An error occurred restoring the virtual machine state during migration. NamespaceMgr could not lock the db file.
```

The destination ESXi host `vmware.log` shows the following messages:

```
[YYYY-MM-DDTHH:MM:SS] In(05) vmx - [msg.checkpoint.migration.failedReceive] Failed to receive migration.
```

```
[YYYY-MM-DDTHH:MM:SS] In(05) vmx - [msg.namespaceMgr.noLock] NamespaceMgr could not lock the db file.
```

The issue is more likely to occur on VMs with hardware version earlier than 19, and impacts only VMs provisioned on shared datastores other than NFS, such as VMFS, vSAN, and vSphere Virtual Volumes.

This issue was reported as known in KB 369767 and is resolved in this release.

esx-update_7.0.3-0.130.24411414

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.130.24411414 • VMware_bootbank_esx-update_7.0.3-0.130.24411414
PRs Fixed	N/A
CVE numbers	N/A

Due to their dependency on the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `loadesx` and `esx-update` .

ESXi-7.0U3r-24411414-standard

Profile Name	ESXi-7.0U3r-24411414-standard
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom, Inc.
Release Date	Dec 12, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_bmcal_7.0.3-0.130.24411414 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.130.24411414 • VMware_bootbank_vdfs_7.0.3-0.130.24411414 • VMware_bootbank_cpu-microcode_7.0.3-0.130.24411414 • VMware_bootbank_gc_7.0.3-0.130.24411414 • VMware_bootbank_vsanhealth_7.0.3-0.130.24411414 • VMware_bootbank_trx_7.0.3-0.130.24411414 • VMware_bootbank_crx_7.0.3-0.130.24411414 • VMware_bootbank_esx-xserver_7.0.3-0.130.24411414 • VMware_bootbank_vsan_7.0.3-0.130.24411414 • VMware_bootbank_native-misc-drivers_7.0.3-0.130.24411414 • VMware_bootbank_esxio-combiner_7.0.3-0.130.24411414 • VMware_bootbank_esx-base_7.0.3-0.130.24411414 • VMware_bootbank_loadesx_7.0.3-0.130.24411414 • VMware_bootbank_esx-update_7.0.3-0.130.24411414
PRs Fixed	3459675
Related CVE numbers	N/A

This patch updates the following issue:

vSphere vMotion tasks fail with an error NamespaceMgr could not lock the db file

In rare cases, when virtual machines are configured with namespaces, an issue with the namespace database might cause migration of such VMs with vSphere vMotion to fail. In the vSphere Client, you see errors such as:

```
Failed to receive migration. The source detected that the destination failed to resume.
```

```
An error occurred restoring the virtual machine state during migration. NamespaceMgr could not lock the db file.
```

The destination ESXi host `vmware.log` shows the following messages:

```
[YYYY-MM-DDTHH:MM:SS] In(05) vmx - [msg.checkpoint.migration.failedReceive] Failed to receive migration.
```

```
[YYYY-MM-DDTHH:MM:SS] In(05) vmx - [msg.namespaceMgr.noLock] NamespaceMgr could not lock the db file.
```

The issue is more likely to occur on VMs with hardware version earlier than 19, and impacts only VMs provisioned on shared datastores other than NFS, such as VMFS, vSAN, and vSphere Virtual Volumes.

This issue was reported as known in KB 369767 and is resolved in this release.

ESXi-7.0U3r-24411414-no-tools

Profile Name	ESXi-7.0U3r-24411414-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom, Inc.
Release Date	Dec 12, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_bmcal_7.0.3-0.130.24411414 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.130.24411414 • VMware_bootbank_vdfs_7.0.3-0.130.24411414 • VMware_bootbank_cpu-microcode_7.0.3-0.130.24411414 • VMware_bootbank_gc_7.0.3-0.130.24411414 • VMware_bootbank_vsanhealth_7.0.3-0.130.24411414 • VMware_bootbank_trx_7.0.3-0.130.24411414 • VMware_bootbank_crx_7.0.3-0.130.24411414 • VMware_bootbank_esx-xserver_7.0.3-0.130.24411414 • VMware_bootbank_vsan_7.0.3-0.130.24411414 • VMware_bootbank_native-misc-drivers_7.0.3-0.130.24411414 • VMware_bootbank_esxio-combiner_7.0.3-0.130.24411414 • VMware_bootbank_esx-base_7.0.3-0.130.24411414 • VMware_bootbank_loadesx_7.0.3-0.130.24411414 • VMware_bootbank_esx-update_7.0.3-0.130.24411414
PRs Fixed	3459675
Related CVE numbers	N/A

This patch updates the following issue:

vSphere vMotion tasks fail with an error NamespaceMgr could not lock the db file

In rare cases, when virtual machines are configured with namespaces, an issue with the namespace database might cause migration of such VMs with vSphere vMotion to fail. In the vSphere Client, you see errors such as:

```
Failed to receive migration. The source detected that the destination failed to resume.
```

```
An error occurred restoring the virtual machine state during migration. NamespaceMgr could not lock the db file.
```

The destination ESXi host `vmware.log` shows the following messages:

```
[YYYY-MM-DDTHH:MM:SS] In(05) vmx - [msg.checkpoint.migration.failedReceive] Failed to receive migration.
```

```
[YYYY-MM-DDTHH:MM:SS] In(05) vmx - [msg.namespaceMgr.noLock] NamespaceMgr could not lock the db file.
```

The issue is more likely to occur on VMs with hardware version earlier than 19, and impacts only VMs provisioned on shared datastores other than NFS, such as VMFS, vSAN, and vSphere Virtual Volumes.

This issue was reported as known in KB 369767 and is resolved in this release.

ESXi7.0U3r - 24411414

Name	ESXi
Version	ESXi7.0U3r - 24411414
Release Date	DEC 12, 2024
Category	Bugfix
Affected Components	• ESXi Component - core ESXi • ESXi Install/Upgrade
PRs Fixed	3459675
Related CVE numbers	N/A

This patch resolves the issues listed in ESXi_7.0.3-0.130.24411414.

Known Issues from Previous Releases

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Corrupted VFAT partitions from a vSphere 6.7 environment might cause upgrades to ESXi 7.x to fail

Due to corrupted VFAT partitions from a vSphere 6.7 environment, repartitioning the boot disks of an ESXi host might fail during an upgrade to ESXi 7.x. As a result, you might see the following errors:

When upgrading to ESXi 7.0 Update 3l, the operation fails with a purple diagnostic screen and/or an error such as:

- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to calculate size for temporary Ramdisk: <error>.`
- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to copy files to Ramdisk: <error>.`
  If you use an ISO installer, you see the errors, but no purple diagnostic screen.

When upgrading to an ESXi 7.x version earlier than 7.0 Update 3l, you might see:

- Logs such as `ramdisk (root) is full` in the `vmkwarning.log` file.
- Unexpected rollback to ESXi 6.5 or 6.7 on reboot.
- The `/bootbank` ,`/altbootbank` , and ESX-OSData partitions are not present.

Workaround: You must first remediate the corrupted partitions before completing the upgrade to ESXi 7.x. For more details, see VMware knowledge base article 91136.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the requirement cannot be satisfied within the ImageProfile. Please refer to the log file for more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in

the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
 The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
 Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s)`.

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU`.

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer`.

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network.` This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi

6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Set-VMHostService -policy "off"$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx` , the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1` .

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set
--tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer":
{ "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"` , run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `“runtime.hardwareStatusInfo.storageStatusInfo”` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.

- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command:
   `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command:
   `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command:
   `esxcli network firewall load.`
5. Start the hostd service by using the command:
   `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats` , you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835` .

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0` .

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set` **-o** `/USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.
2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

vSAN Issues

PR 2962316: vSAN File Service does not support NFSv4 delegations

vSAN File Service does not support NFSv4 delegations in this release.

Workaround: None

PR 3235496: Applications on a vSAN cluster become intermittently unresponsive

If the advanced option `preferHT` is enabled on an AMD server in a vSAN cluster, the virtual CPUs of a virtual machine run on the same last level cache. When the virtual CPUs are all very busy and an NVMe thread to handle I/Os happens to run also on the same last level cache, the NVMe thread takes very long to complete, because it competes for CPU resources with the busy VMs. As a result, the I/O latency is very high and might lead to intermittent unresponsiveness of storage and applications on the vSAN cluster. In the backlog, you see errors such as `Lost access to volume <uuid> due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.`

Workaround: Use the command `esxcli system settings advanced set -o /Misc/vmknvmeCwYield -I 0` to avoid competition between the NVMe completion queue and busy virtual CPUs.

VMware ESXi 7.0 Update 3q Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Product Support Notices
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues

Introduction

VMware ESXi 7.0 Update 3q | 21 MAY 2024 |Build 23794027 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3q, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3q. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- This release resolves CVE-2024-22273. For more information on this vulnerability and its impact on VMware by Broadcom products, see VMSA-2024-0011.

ESXi 7.0 Update 3q adds support to vSphere Quick Boot for multiple servers, including:

- HPE
  - Alletra Storage Server 4110
  - Alletra Storage Server 4140
  - HPE Cray XD670
  - ProLiant DL110 Gen11

- Dell Inc.
  - MX760c vSAN Ready Node
  - PowerEdge C6615
  - PowerEdge HS5610
  - PowerEdge HS5620
  - PowerEdge XR8610t
  - R7625 vSAN Ready Node
  - VxRail VP-760xa
  - VxRail VS-760
- Cisco Systems Inc.
  - UCSC-C220-M7N
  - UCSC-C240-M7SN
  - UCSX-210C-M7
  - UCSX-410C-M7
- Supermicro
  - SYS-221BT-HNC8R

For the full list of supported servers, see the VMware Compatibility Guide.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3p Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3o Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3n Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3m Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3l Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Product Support Notices

Reduction in the memory usage of the ps command:

In ESXi 7.0 Update 3q, an optimization of memory usage for the pscommand reduces memory required to run the command by up to 96%.

Patches Contained in This Release

This release of ESXi 7.0 Update 3q delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3q-23794027-depot.zip
Build:	23794027
Download Size:	574.6 MB
md5sum:	a22098da50aa15f007a59e3501da8083
sha256checksum:	2ece2ea2b11c1fe03ca432612c042235e29ef60b634b090e4c055c33c7637c38
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.125.23794027	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.125.23794027	Bugfix	Critical
VMware Native AHCI Driver	VMware-ahci_2.0.11-3vmw.703.0.125.23794027	Bugfix	Critical
VMware NVMe over TCP Driver	VMware-NVMeoF-TCP_1.0.0.3-1vmw.703.0.125.23794027	Bugfix	Critical
Network driver for Intel(R) X710/XL710/XXV710/X722 Adapters	Intel-i40en_1.11.1.32-1vmw.703.0.125.23794027	Bugfix	Critical
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.120.23794019	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.120.23794019	Security	Critical
ESXi Tools Component	VMware-VM-Tools_12.3.5.22544099-23794019	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include

all of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:

- VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
- VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
- VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
- VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3q-23794027	Bugfix	Critical	Security and Bugfix
ESXi70U3sq-23794019	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3q-23794027-standard
ESXi-7.0U3q-23794027-no-tools
ESXi-7.0U3sq-23794019-standard
ESXi-7.0U3sq-23794019-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi7.0U3q - 23794027	MAY 21 2024	Bugfix	Security and Bugfix image
ESXi7.0U3sq - 23794019	MAY 21 2024	Security	Security only image

For information about the individual components and bulletins, see the Resolved Issues section.

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.125.23794027

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_gc_7.0.3-0.125.23794027 • VMware_bootbank_esx-xserver_7.0.3-0.125.23794027 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.125.23794027 • VMware_bootbank_esxio-combiner_7.0.3-0.125.23794027 • VMware_bootbank_vdfs_7.0.3-0.125.23794027 • VMware_bootbank_crx_7.0.3-0.125.23794027 • VMware_bootbank_esx-ui_2.13.2-22721163 • VMware_bootbank_esx-base_7.0.3-0.125.23794027 • VMware_bootbank_trx_7.0.3-0.125.23794027 • VMware_bootbank_vsanhealth_7.0.3-0.125.23794027 • VMware_bootbank_cpu-microcode_7.0.3-0.125.23794027 • VMware_bootbank_native-misc-drivers_7.0.3-0.125.23794027 • VMware_bootbank_vsan_7.0.3-0.125.23794027 • VMware_bootbank_bmcal_7.0.3-0.125.23794027
PRs Fixed	3269229, 3336578, 3332098, 3324772, 3337108, 3319535, 3336916, 3331375, 3326805, 3335978, 3267977, 3323978, 3331256, 3332691, 3313970, 3312843, 3309601, 3317598, 3323119, 3326739, 3317618, 3244429, 3328641, 3328638, 3328337, 3326300, 3329238, 3328301, 3297696, 3296093, 3317448, 3285491, 3276174, 3297629, 3314959, 3309482, 3320147, 3297625, 3297729, 3311303, 3297704, 3309472, 3297749, 3298709, 3320949, 3310432, 3297774, 3302255, 3270210, 3311302, 3257098, 3311831, 3309603, 3317088, 3321157, 2964964, 3305227, 3318350, 3256083, 3269969, 3317445, 3314400, 3267704, 2760003, 3313882, 3243360, 3293469, 3284876, 3265330, 3303842, 3303855, 3293093, 3309148, 3307580, 3301661, 3304469, 3260297, 3260070, 3297409, 3252235, 3287748, 3306033, 3273752, 3288607, 3289238, 3284916, 3303694, 3284133, 3273653, 3298508, 3289605, 3289669, 3291198, 3240347, 3280468, 3285518, 3283501, 3275377, 3267449, 3282267, 3256992, 3251790, 3275137, 3240662, 3259035, 3259205, 3266912, 3282224, 3273653, 3346924, 3346935, 3346816, 3237506, 3331539, 3271089, 3291105, 3346938, 3312150, 3388772
CVE numbers	CVE-2024-22273

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the gc, esx-xserver, esx-dvfilter-generic-fastpath, esxio-combiner, vdfs, crx, esx-ui, esx-base, trx, vsanhealth, cpu-microcode, native-misc-drivers, vsan , and bmcal VIBs to resolve the following issues:

PR 3318350: The sfcb service might fail and generate multiple dump files

Due to a NULL reference, the sfcbd service might fail. You see multiple dump core files created at /var/core/sfcb-vmware_bas-zdump .

This issue is resolved in this release.

PR 3317598: A disk in a vSAN cluster might fail without an error and cause unresponsiveness or failure of virtual machines in the cluster

In rare cases, if an I/O is stuck due to a hardware of firmware issue on a disk in a vSAN cluster, and a transient error occurs at the same time, a race between the stuck I/O and the transient error handling might cause a deadlock. vSAN does not process any reports on events after the deadlock and you do not receive any notifications. As a result, virtual machines on the cluster of the affected disk become unresponsiveness or fail without logs or warning.

This issue is resolved in this release.

PR 3273653: In vSphere systems using memory cards larger than 64GB, you might see "Unable to allocate SCSI_Command" log messages

If you use physical memory cards larger than 64GB for your vSphere system, whenever the number of VM count increases, you might see errors for the SCSI command slab and heap allocations such as VSCSI: 590: VSCSI_VmkAccumulateSG failed: Out of memory or Unable to allocate SCSI_Command.

This issue is resolved in this release. The fix applies a scale factor based on the size of the physical memory.

PR 3326739: You do not get debugging logs when the vmkdevmgr service fails

In very rare cases, if the vmkdevmgr service fails and core dumps are not enabled, you might not get debugging logs that help you to identify the underlying issue for the failure.

This issue is resolved in this release. The fix adds an automatic check if core dumps for the vmkdevmgr service are enabled.

PR 3309601: The vSphere Virtual Volumes service might fail with a dump while applying a VM Policy to a VM on an ESXi host

In the rare case when an untracked reference to a vendor provider parameter in a vSphere API for Storage Awareness (VASA) session is accessed after deletion, it might cause dump generation. As a result, the vSphere Virtual Volumes service might fail with a dump while applying a VM Policy to a VM on an ESXi host.

This issue is resolved in this release.

PR 3265330: The VMX service might fail during migration of virtual machines with vSphere Virtual Volumes if the volume closure on the source takes long

In some scenarios, such as virtual machines with vSphere Virtual Volumes and Changed Block Tracking (CBT) or Content Based Read Cache (CBRC) enabled, during storage migration, flushing pending I/Os on volume closure at the source might take long, like 10 sec. If clearing the pending I/Os is not complete by the time the VMX service tries to reach the volumes on the destinations host, the service fails.

This issue is resolved in this release. The fix makes sure that all vSphere Virtual Volumes and disks are closed on the source host before the destination host tries to open them.

PR 3331375: Path to SATA drives might move to permanently lost state during a secure wipe operation

During a secure wipe operation, some SATA drives might not provide proper vital product data (VPD) to queries from the host. As a result, the HPP plug-in might incorrectly interpret changes in the physical media and mark a path for the SATA device as permanently lost.

This issue is resolved in this release.

PR 3328638: An ESXi host might fail with a purple diagnostic screen when probe I/Os fail with a retriable error for a long time

In rare scenarios, if for a long period an adapter or device continues to retry an operation that has failed due to a short-lived disruption such as a transient device error or controller reset, a CPU lockup might occur. As a result, an ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3293469: In the vSphere Client, you see a flat line in the read/write IO latency stats for a vSphere Virtual Volumes datastore

In the vSphere Client, when you navigate to **Monitor >Advanced >Datastore** to see the advanced performance metrics of a virtual machine, you might see a flat line in the read/write I/O latency stats for a vSphere Virtual Volumes datastore. The issue occurs due to incorrect calculation of the counters for the read/write I/O latency as a cumulative average.

This issue is resolved in this release.

PR 3303842: WRITE SAME (16) commands with the unmap bit set fail on thick disks

If information from the VPD Page B2 does not prevent the guest OS from activating the unmap bit in a `WRITE SAME (16)` command on thick disks, the command expectedly fails in a vSphere environment. In addition, if the guest OS does not receive a proper error code, it keeps issuing unmap requests by using `WRITE SAME (16)` , also called block zeroing, and this causes I/O errors.

This issue is resolved in this release. With the fix, VPD Page B2 returns proper reports for `WRITE SAME (16)` with unmap support and the guest OS receives a proper error code when unmap is not supported, to prevent unnecessary unmap attempts by the guest.

PR 3314400: An ESXi host fails with a purple diagnostic screen and message @BlueScreen: NMI IPI: Panic requested by another PCPU

In vSphere environments with NSX Data Center, an additional sanity check of the vmxnet3 driver might cause a port or portset lock that might lead to a lock contention. As a result, an ESXi host might fail with a purple diagnostic screen and message `@BlueScreen: NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release. The fix removes the unnecessary vmxnet3 driver check.

PR 3346924: Upgrade of VMware NSX fails due to a stale DVSPORT_FLAG_RESERVED flag

In very rare cases, a failed vSphere vMotion task might keep a `DVSPORT_FLAG_RESERVED` flag on a port and prevent upgrades of VMware NSX, because the switch on which the port resides cannot be removed. Only a restart of the ESXi host can clean the flag.

This issue is resolved in this release.

PR 3243360: You do not see ESXi host names in the Integrated Dell Remote Access Controller (iDRAC)

When you run the command `localcli hardware ipmi bmc get` in an iDRAC environment, some of the fields for ESXi host names are empty.

This issue is resolved in this release. The fix updates the IPMI BMC hostname during static IP configuration, when the ESXi host is statically configured and rebooted.

PR 3289605: Deactivated transmit queuing option might prevent you from optimizing networking performance

If the `NetSchedHClkVnicMQ` advanced option for transmit queuing is not active, a VNIC with multiple queues might not be able to utilize all queues and prevent significant enhancement of the throughput.

This issue is resolved in this release. The fix makes the `NetSchedHClkVnicMQ` option active by default.

PR 3346935: Migration of virtual machines might fail when vSphere Network I/O Control is active on an ESXi host port to which container ports are mapped to

In rare cases, migrating virtual machines might fail when vSphere Network I/O Control is active on an ESXi host port to which container ports are mapped to, because a dummy port is created at the destination host.

This issue is resolved in this release.

PR 3301661: An I/O filter provider might show offline because of IOFilterVP memory leak

Due to a memory leak in IOFilterVP, an I/O filter provider for an ESXi host might show offline in the vSphere Client under **Configure** > **Storage**. The issue occurs because the SSL cache might consume all heap memory to process VASA API requests.

This issue is resolved in this release. The fix adds a timeout for SSL caching sessions to prevent the memory leak.

PR 3346816: You cannot update the VIB for the NVIDIA GRID vGPU graphics card without rebooting the ESXi host

In case the VIB for the NVIDIA GRID vGPU graphics card is large, lack of sufficient space allocated for the kernel module might prevent automatic update and the operation requires a manual reboot of the ESXi host to complete.

This issue is resolved in this release.

PR 3309482: vSAN host fails with purple diagnostic screen during reboot or mounting a vSAN disk group

A rare issue might cause an incorrect initialization of an internal attribute of a component during recovery of the vSAN logical log, LLOG. As a result, the vSAN host might fail with purple diagnostic screen and in the logs you see an error such as:

```
VMK_ASSERT(cfDisableAssert || LSNEntryLessThan(entry, cfParams->gcpEntry))
```

This issue is resolved in this release.

PR 3306033: You need to manually open the firewall at ports that are different from the default 514 for TCP/UDP and 1514 for SSL protocols

Starting with ESXi 7.0 Update 3q, when you configure syslog remote hosts, or loghosts, with non-standard ports, the vmsyslogd service automatically creates persistent dynamic firewall rules. You no longer need to manually open the firewall at ports that are different from the default 514 for TCP/UDP and 1514 for SSL protocols respectively. When configuring remote hosts with the standard ports, you still need to enable the syslog firewall ruleset.

This issue is resolved in this release. For more information, see Opening the firewall for syslog emission to remote hosts.

PR 3282267: The hostd service might intermittently fail due to an invalid sensor data record

In rare cases, the Baseboard Management Controller (BMC) might provide an invalid sensor data record to the hostd service and cause it to fail. As a result, ESXi hosts become unresponsive or disconnect from vCenter.

This issue is resolved in this release. The fix implements checks to validate the sensor data record before passing it to the hostd service.

PR 3237506: What If analysis on vSAN Capacity screen shows incorrect values when using RAID5 or RAID6 storage policy

In vSAN cluster **Capacity** screen, the What If analysis might show incorrect free space when the cluster is using a RAID5 or RAID6 storage policy.

This issue is resolved in this release.

PR 3276174: vSphere vMotion operations between ESXi 7.x hosts fail with the error "Destination failed to preopen disks"

If on an ESXi 7.x host you use an older Virtual Volumes storage provider, also called a VASA provider, it might not allow binding multiple vSphere Virtual Volumes in batches to optimize the performance of migration and power on. As a result,

in the vSphere Client you might see the error `Destination failed to preopen disks` when running vSphere vMotion operations between 7.x hosts.

This issue is resolved in this release.

PR 3311831: ESXi hosts intermittently fail with a purple diagnostic screen and the error "Spin count exceeded - possible deadlock"

Due to a rare issue with packets that might be out of order in a TCP connection, you might see ESXi hosts intermittently to fail with a purple diagnostic screen and the error `Spin count exceeded - possible deadlock`. In the `vmkernel.log` file, you see a backtrace for errors in the tcpip stack such as:

```
2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bbf0:
[0x42003081b976]Lock_CheckSpinCount@vmkernel#nover+0x26f stack: 0xffffffffffffffff8,
0x15a8f9ed9da6c33, 0x3ff, 0x43201ac1efd8, 0x1

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bc40:
[0x420030908c8d]SP_WaitReadLock@vmkernel#nover+0xba stack: 0x43201ac1efd8, 0x43201ac1efdc,
0x0, 0x0, 0x41ffd380b7a0

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bc80:
[0x420030908d2a]SPAcqWriteLockWork@vmkernel#nover+0x33 stack: 0x43201ac10f60,
0x420031ce1595, 0x43201cac3b80, 0x420031d4da3b, 0x43201cac3b80

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bca0:
[0x420031ce1594]rw_wlock@(tcpip4)#<None>+0x8d stack: 0x43201cac3b80, 0x41ffd38030b0, 0x6,
0x41ffd380b7a0, 0x43201ac10f60

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bcb0:
[0x420031d4da3a]tcp_usr_attach@(tcpip4)#<None>+0x7b stack: 0x6, 0x41ffd380b7a0,
0x43201ac10f60, 0x43201ac1aff0, 0x453c10e1bd58

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bcf0:
[0x420031cff0a6]socreate@(tcpip4)#<None>+0x1fb stack: 0x58, 0x43201ac1aff0,
0x41ffd380b7a0, 0x1, 0x6

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bd40:
[0x420031ceb2b6]vmk_socket@(tcpip4)#<None>+0xa3 stack: 0x1, 0x420031ccf047,
0x45dbc1758950, 0x4313d2803210, 0x43201ac01700
```

This issue is resolved in this release.

PR 3252235: ESXi hosts might fail to boot due to a rare deadlock between open and rename operations on objects with parent-child relationship

A rename operation locks the source and destination directories based on the object pointer address with the assumption that the parent object has the lower address. In rare cases, the assumption might not be correct and the rename lock can happen for the child first and then the parent, while the open operation locks the parent first and then the child. As a result, a deadlock between the open and rename operations occurs and ESXi hosts fail to boot.

This issue is resolved in this release.

PR 3313970: ESXi hosts might fail with a purple diagnostic screen due to a write lock of the uplink watchdog

During a regular sanity check, the uplink watchdog might hold a write lock that prevents reads from other services and might cause the ESXi host might fail with a purple diagnostic screen. In the backtrace, you see errors such as:

```
Panic Message: @BlueScreen: NMI IPI: Panic requested by another PCPU. RIPOFF(base):RBP:CS

[0x14e1e0(0x420033000000):0x430201d03440:0xf48] (Src 0x4, CPU14).
```

This issue is resolved in this release. The fix replaces the write lock with a read lock for regular sanity checks.

PR 3331539: Migration between NSX segments with many container logical ports might cause an ESXi host to fail with a purple diagnostic screen

A rare race condition between vSphere vMotion tasks on NSX Segments with many container logical ports might cause an ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3240662: Host Profile compliance check throws incorrect error message "IPv4 vmknic gateway configuration doesn't match the specification"

In the vSphere Client, you might see the error `IPv4 vmknic gateway configuration doesn't match the specification` when running a compliance check on a Host Profile. The error remains even when you remediate the Host Profile. However, the default gateway settings are defined from the Host Customization workflows and you should not see such an error message during compliance checks. Disregard the message, as it does not affect the host profile functions.

This issue is resolved in this release.

PR 3271089: Virtual machines with a lightweight delta (LWD) snapshot might fail to start after a failure of the vmx service

In rare cases, if the vmx service fails during the creation of a LWD snapshot, some partially initialized LWD snapshot files might remain on the datastore. As a result, virtual machines with such LWD snapshots might fail to start due to validation failures.

This issue is resolved in this release.

PR 3304469: vSphere vMotion operations might fail due to a rare issue with no namespaces present in the namespacemgr.db file

When a virtual machine is configured with namespaces and for some reason the namespaces table in the `namespacemgr.db` file is empty in the ESXi host database, migration of such a VM by using vSphere vMotion might fail. In the `vmware.log` file, you see errors such as:

```
vmx - NamespaceMgrCheckpoint: No valid queue found while restoring the namespace events.
The migrate type is 1.
```

This issue is resolved in this release.

PR 3291105: While detaching an Enhanced Networking Stack (ENS) port from an ESXi host, the host might fail with a purple diagnostic screen

During deactivation of ENS in scenarios such as an upgrade or a VNIC configuration change, while detaching an ENS port from an ESXi host with active ENS, the port might be removed from the port list and not be available for further reference, which might cause an invalid memory access error. As a result, the ESXi host fails with a purple diagnostic screen.

This issue is resolved in this release.

PR 3346938: After a NSX Distributed Security installation, vSphere vMotion might not restore a switch security filter on the destination side

When you opt to install the Security Only option of NSX Distributed Security, vSphere vMotion might not restore a switch security filter on the destination side and the Address Resolution Protocol (ARP) fails.

This issue is resolved in this release.

PR 3312150: Failover of VMs on vSphere Virtual Volume datastores might fail due to wrong order of metadata from vSphere API for Storage Awareness (VASA) provider

Certain VASA providers might return metadata info in a different order than what an ESXi host requests. As a result, when VMs on a vSphere Virtual Volume datastore fail over to a recovery site, the VMs cannot reboot on the target site.

This issue is resolved in this release. With the fix, even if a VASA provider returns metadata info in a different order from the ESXi host request, failover succeeds.

PR 3328641: An ESXi host might fail with a purple diagnostic screen due to a rare issue during a read-modify-write (RMW) operation

On 512e software emulated devices, when I/O requests are not multiple of 4096, ESXi runs RMW operations. In such cases, the final write I/O issue path can access the write command frame after the write is issued to the target. If the target completes the write request before the issue path accesses the write frame, the write frame is freed. As a result, you might see a Use-After-Free scenario that might lead to failure of the ESXi host with a purple diagnostic screen.

This issue is resolved in this release.

PR 3332098: Asynchronous write operations to a SMB file share on the vSAN File Service might cause data transfer issues

In rare cases, a race condition during asynchronous write operations to a SMB file share on the vSAN File Service might cause data transfer issues such as truncation.

This issue is resolved in this release.

PR 3256992: vSphere vMotion tasks fail for VMs on port groups with promiscuous mode enabled

A rare issue with corrupted network packets that becomes evident in secure network protocols, where packet data integrity is checked upon receipt, might lead to connectivity issues on port groups with promiscuous mode enabled. As a result, you might see vSphere vMotion tasks failing for VMs on such port groups. You see data integrity errors such as `Failed to decrypt ciphertext` in the backtrace.

This issue is resolved in this release.

PR 3244429: Exit Code 127 error in the hostd service might cause an ESXi host to disconnect temporarily from vCenter

Due to an issue in the open source glibc components, attempts by hostd to process the list of installed I/O filters on an ESXi host might intermittently cause an Exit Code 127 error. In the `/var/run/log/syslog.log` , you see lines such as:

```
2022-10-13T08:00:20.180Z watchdog-hostd[<PID>]: 'hostd ++min=0,swapscope=system' exited after X seconds 127
```

As a result, the ESXi host temporarily disconnects from vCenter until the hostd watchdog restarts the service and connectivity restores. The issue has been observed while loading the `vmwarelwd` I/O filter.

This issue is resolved in this release. ESXi 7.0 Update 3q adds a hostd configuration option that allows you to deactivate an I/O filter without removing it from the vCenter system and skip reporting such filters in the host configuration overhead. To use the option, log in to SSH and complete the following steps:

1. Set the `plugins/hostsvc/report_disabled_filters_in_host_config` option in the hostd configuration to `False` as described in VMware knowledge base article 82227.
2. Deactivate the `vmwarelwd` filter by running the following python script directly on the host:
   ```
   import vmware.vsi as vsi
   vsi.set('/iofilters/statusDisabledEvent', {'filterName': 'vmwarelwd', 'failureReason' : 'workaround'})
   ```

PR 3332691: vSAN IOPS performance data not available for VM multi-writer virtual disk

The following performance charts for a vSAN VM multi-writer virtual disk, under **Monitor** > **vSAN** > **Performance** > **Virtual Disks**, are not available: IOPS, IOPS limit, and Delayed Normalized IOPS. These charts are available only for disks without active multi-writer mode.

This issue is resolved in this release.

PR 3288607: An ESXi host might fail with a purple diagnostic screen due to a rare storage heap corruption in NVMe devices

In rare cases, an I/O thread from a NVMe device, such as deleting a virtual machine from a datastore using NVMe devices, might complete before the High-Performance Plug-in (HPP) claims the device to complete the thread. As a result, HPP tries to access a non-existing thread which leads to a failure of the ESXi host with a purple diagnostic screen and an error such as `PSOD @BlueScreen: PANIC bora/vmkernel/main/dlmalloc.c:4763`.

This issue is resolved in this release.

PR 3273752: ESXi hosts fail with a purple diagnostic screen and a #PF Exception 14 in world 2097479:HELPER_SCSI_ error

After a change in the namespace list for a controller, for example the PsaNvmeController, the update semaphore works as expected, but the change might not complete because no lock is available. As a result, the ESXi host fails with a purple diagnostic screen and a `#PF Exception 14 in world 2097479:HELPER_SCSI_ error`.

This issue is resolved in this release.

PR 3267977: You might see spikes in the latency performance metrics after creating a virtual machine disk snapshot

After you create a virtual machine disk snapshot, you might see latency spikes in the vSphere performance charts. Such unusual spikes are due to the recreation of some internal system objects and the restart of the latency performance counters in the storage subsystem.

This issue is resolved in this release. The fix prevents false latency alarms after taking virtual machine disk snapshots.

PR 3305227: If you do not increase the TCP/IP heap memory limit before installation of NSX-T Data Center kernel modules, ESXi hosts might crash

When you install NSX-T Data Center kernel modules on ESXi hosts with high loads, the pre-allocated TCP/IP heap during boot required for the operation might not be sufficient and cause the ESXi host to fail with a purple diagnostic screen. The issue occurs when the TCP/IP heap cannot grow quickly enough to provide a continuous allocation of 2 MB of memory in case of memory fragmentation on such ESXi hosts. As a result, ESXi hosts might fail with a purple diagnostic screen and a `vmkernel.log` error such as

```
Heap: 3707: Heap tcpip (44384680/1073746344): Maximum allowed growth (1048576) too small for size (1203496)
```

The purple diagnostic screen failure is less likely to occur if you put the ESXi host in maintenance mode before the NSX-T Data Center kernel modules installation, as MM significantly reduces the memory pressure.

This issue is partially resolved in this release. Starting from ESXi 7.0 Update 3, if you are planning an NSX-T Data Center installation, you can increase the `TcpipHeapSize` limit pre-allocated during boot to 128 MB. For example, if you want to increase the `TcpipHeapSize` allocation to the maximum, you can use the following steps:

1. Increase the heap size to 128 MB by using the command `esxcfg-advcfg -s 128 /Net/TcpipHeapSize`
2. Confirm that the heap size is 128 MB: `esxcfg-advcfg -g /Net/TcpipHeapSize`
3. Reboot the ESXi host.

To avoid this issue, you can reboot the ESXi host and install NSX-T Data Center with no VMs running.

PR 3328301: ESXi hosts might fail with a purple diagnostic screen due to a race condition in the High Performance Plug-in (HPP)

Due to a rare race condition in HPP, when a storage path failover and device deletion occur at the same time, ESXi hosts might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3257098: A virtual machine fails with McastFilter_Deactivate error

In very rare cases, when a VM is low on memory, a code path might not initialize all its members on restart and cause the VM to fail with a purple diagnostic screen and an error such as `McastFilter_Deactivate`.

This issue is resolved in this release. Avoid low memory state of VMs to prevent similar issues.

PR 3317448: IPv6 routing disappears after you deactivate router advertisement on an ESXi host and the host loses connectivity

Deactivating IPv6 router advertisements (RA) on the physical network or deselecting the option "Obtain IP Address through Router Advertisement" at the VMkernel level might cause the default route for the VMkernel adapter to disappear, even when you have a static IPv6 address on the adapter. The issue occurs only when the IPv6 prefix of both the static IP address and the prefix specified in the RA message are the same. As a result, ESXi incorrectly removes the route entry for that particular subnet, despite that the static IP address is still active for the same prefix, and the ESXi host loses connectivity.

This issue is resolved in this release. Avoid using the same IPv6 prefix for both a static IP address and addresses that are automatically configured in RA messages to prevent the issue.

PR 3312843: ESXi hosts intermittently disconnect from the vCenter system and the hostd service restarts

If an ESXi host uses only one of the multipath plug-ins, either HPP or NMP, when the hostd service collects telemetry data on scheduled intervals, the call might return a null pointer value. Dereferencing the `nullptr` might lead to a hostd failure, but the service automatically restarts. As a result, you see the ESXi host intermittently disconnected from the vCenter system.

This issue is resolved in this release. The fix adds a `nullptr` check.

PR 3328337: The hostd service might become unresponsive after a restart due to a rare issue with Inter Process Communication (IPC)

If an IPC process has incorrect payload in the IPC packet, for example: an incorrect version in the header, a deadlock in the iSCSI daemon might cause the hostd service to become unresponsive after a hostd restart. As a result, you cannot perform any operations on the affected ESXi host and VMs by using the vSphere Client.

This issue is resolved in this release.

PR 3285491: You cannot use host profiles to configure a path selection policy for disks using Raw Device Mapping

In some cases, when you try to change or configure the path selection policy of multiple virtual machines by using a host profile, the operation fails for VMs using Raw Device Mapping.

This issue is resolved in this release.

PR 3296093:ESXi hosts intermittently fail with a purple diagnostic screen and a PF Exception 14 error

While running an ESXi upgrade, a rare race condition in the device registration during disk initialization might lead to an ESXi host failing with a purple diagnostic screen. In the screen, you see an error such as `@BlueScreen: #PF Exception 14 in world XXXXX:HELPER_SCSI_ IP` and in the backtrace, you see `vmk_ScsiGetDeviceState` and `nmp_DeviceUpdatePathStates`.

This issue is resolved in this release.

PR 3321157: You might see network outages in vSphere systems using Intel i40en physical NICs and with Enhanced data path enabled

On Intel i40en NICs, TSO packets that exceed the Maximum Segment Size (MSS) of 8 segments might cause the NIC to become unresponsive. In rare cases, a TSO packet from a VM or from a vmknic might exceed the 8-segement limit and you might see network outages due to blocked pNIC tx traffic. The issue is more likely to occur in vSphere systems using Intel i40en physical NICs and with Enhanced data path enabled.

This issue is resolved in this release.

PR 3307580: Large TCP segmentation offload (TSO) packets might cause network traffic latency and intermittent loss of connectivity for some virtual machines

Environments with the enhanced data path networking stack mode enabled might see network traffic latency and intermittent loss of connectivity for some virtual machines due to an issue with the handling of large TSO packets.

This issue is resolved in this release.

PR 3275137: Rare data corruption issue in vSphere systems that use service insertion might lead to ESXi host failure

In vSphere systems that use service insertion, an error with the check of the available buffer size before pulling data might lead to data corruption that might cause the ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release. The fix makes sure that data pull during service insertion runs only if a sufficient buffer exists.

PR 3270210: The Busybox shell on an ESXi host might fail after you disable echo mode

If you enter a command after `stty -echo` , which disables the echo mode on a Busybox sh shell on an ESXi host, the shell might fail with a coredump.

This issue is resolved in this release.

PR 3319535: Virtual machines with independent_nonpersistent disks might become inaccessible after a VM reset

During a reset, a virtual machine with independent_nonpersistent disks deletes existing redo log files and creates a new redo log. The vmx process updates the new .redo settings in-memory, not in the .vmx file, and when the hostd service reads the disk properties from the .vmx file during sync up, it might consider the redo logs inconsistent. As a result, hostd marks the VM as invalid and the VM becomes inaccessible.

This issue is resolved in this release.

PR 3317445: Enhanced Network Datapath (EDP) might reserve too much memory on a large vSphere system and cause resource issues

EDP reservation is linear to the total memory by reserving up to 1.6% of the total. For a VM with high memory reservation in a large vSphere system, such a memory buffer might be too big. For example, if the system has a 100TB of memory, the EDP reservation might be 1.6TB. As a result, you might see resource issues such as not being able to hot-add VNICs to VMs with high memory reservation.

This issue is resolved in this release. The fix sets the EDP reservation limit at 1% of the total memory and puts a 5GB cap on a single memory reservation. You can adjust the memory reservation limit by using the VMKernel boot option `ensMbufPoolMaxMinMB` or by using the following command: `esxcli system settings kernel set -s ensMbufPoolMaxMBPerGB -v <value-in-MB>` . In any case, you must reboot the ESXi host to enable the change.

PR 3283501: SFCB start, stop, and reporting operations fail due to a stale lockfile: /var/run/sfcbd-init.lock

In rare cases, the `sfcbd-init` script, which creates a lockfile `/var/run/sfcbd-init.lock` to prevent multiple instances of the script from running at the same time, receives a SIGPIPE signal, which terminates the script and leaves the lockfile unhandled. As a result, any further attempts to run the script fail because they cannot acquire the lock.

This issue is resolved in this release. The fix adds SIGPIPE to the list of signals handled by the trap command in the `sfcbd-init` script. This ensures that the lock file is cleared even when the script receives a SIGPIPE signal.

PR 3285243: If an NFS server sends a file handle with 0 length during a new directory creation, ESXi hosts might fail with a purple diagnostic screen

On volumes mounted by using NFSv4.1, if the NFS server sends a file handle with length of 0 in response to a new directory request, the ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3317088: You see slow response times in vSphere environments with NVMe SSDs

When a NVMe SSD fails, it does not respond to any commands from the NVMe driver, such as closing outstanding I/Os. As a result, many I/O and NVMe driver commands might remain pending and cause slow response times in the vSphere environment or even failure of upper layer applications.

This issue is resolved in this release. With the fix, the NVMe driver initiates controller or queue reset in case driver commands are not effective, to allow closing of outstanding I/Os.

PR 3302202: You might see placeholders listed in the Guest OS version drop-down menu for new ESXi virtual machines

When creating a new virtual machine, in the **Guest OS version** drop-down menu you might see placeholders such as Windows 12 and Windows Server 2025. You cannot use such placeholders to create new virtual machines.

This issue is resolved in this release.

PR 3289669: You cannot power on a virtual machine after a failed or canceled export of an Open Virtual Format (OVF) file

A rare deadlock caused by a failed or canceled export of a VM as an OVF file might prevent subsequent start of that VM. The VM appears in a **VM_STATE_EXPORTING** state.

This issue is resolved in this release. If the export of an OVF file fails due to a network outage, you cannot prevent the issue, but you can avoid it if you do not manually cancel OVF exports. If you already face the issue, restart the hostd service on the affected ESXi host by either using the SSH command `/etc/init.d/hostd restart` or selecting **Restart Management Agents** under **Troubleshooting options** in the Direct Console User Interface. The restart of the host service stops any operations on the ESXi host.

PR 3313882: Virtual machines and data objects might become inaccessible after an ESXi firewall refresh

In some scenarios, a refresh of the ESXi firewall on vSAN clusters might refer to an incomplete object in the ESXi Configuration Store (ConfigStore) and cause the Reliable Datagram Transport (RDT) and Cluster Monitoring, Membership and Directory Service (CMMDS) firewall rules to be disabled. As a result, some clusters might be isolated and virtual machines and data objects might become inaccessible.

This issue is resolved in this release.

PR 3280714: In the web console of Linux virtual machines, the Caps Lock option does not work consistently

When you enable the Caps Lock option in the web console of a Linux virtual machine, the typing output might not consistently be capital letters.

This issue is resolved in this release.

PR 3287440: ESXi hosts stop responding to tasks from the vSphere Client

Due to a rare race condition with accessing vSphere Distributed Switch data from competing services, ESXi hosts might stop responding to tasks from the vSphere Client. For example, in NSX Data Center for vSphere environments, you might see an error such as `TN Profile attachment to the cluster is in progress` that prevents you from running other tasks.

This issue is resolved in this release.

PR 3282224: VXLAN traffic generated from a guest VM to port 4789 fails

ESXi hosts have VXLAN port 8472 enabled by default and not the UDP port 4789, which is the default for NSX 6.2.3 and later. As a result, traffic to VXLAN port 4789 fails.

This issue is resolved in this release. The fix adds port 4789 to the list of VXLAN ports by default.

PR 3260070: ESXi hosts might fail with a purple diagnostic screen due to a NULL pointer reference in a tardisk object

A NULL pointer violation with `VisorFSTarDoIOInt()` in the backtrace might cause ESXi hosts to fail with a purple diagnostic screen. The issue occurs in the following conditions:

1. A vSphere admin manually logs into the host by using SSH
2. Modifies a tardisk file, for example in `/etc` , without re-writing the file completely
3. Performs an upgrade that replaces a VIB containing that specific file
4. The admin or an ESXi service access the modified file

This issue is resolved in this release.

PR 3284133: ESXi hosts in environments with NVMe PCIe devices might temporarily lose connectivity during collection of diagnostic information

When you use the `vm-support` command to collect information about ESXi systems such as network, storage, and vSAN, logs for the telemetry and persistent events of NVMe PCIe controllers are temporally stored in the ramdisk `/tmp` directory. If your system has many NVMe PCIe devices or the log file is large, the ramdisk `/tmp` directory quickly becomes full. As a result, ESXi hosts in environments with NVMe PCIe devices might temporarily lose connectivity until the `vm-support` collection completes.

This issue is resolved in this release. The fix selects the VMFS datastore with the most free space to store `nvme` logs and compresses each log file to save storage space.

PR 3275377: VBS-enabled Windows VMs might intermittently fail with a blue diagnostic screen on ESXi hosts running on AMD processors

Windows virtual machines with virtualization-based security (VBS) enabled might intermittently fail with a blue diagnostic screen on ESXi hosts running on AMD processors. The BSOD has the following signature:

```
SECURE_KERNEL_ERROR (18b)The secure kernel has encountered a fatal error.
Arguments:
Arg1: 000000000000018c
Arg2: 000000000000100b
Arg3: 0000000000000000
Arg4: 000000000000409b
```

This issue is resolved in this release.

PR 3259205: A stateless ESXi host might lose connection to vCenter after a reboot

During the boot of a stateless ESXi host, in very rare situations, the management vmknic might change unexpectedly and change the IP address of the host. As a result, the host disconnects from vCenter. If you apply a host profile, in the vSphere Client you might see an error such as **Host profile apply failed with error: Error: A specified parameter was not correct: SelectVnic.vnic.Specification.NetStackInstanceKey.**

This issue is resolved in this release.

esx-update_7.0.3-0.125.23794027

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-update_7.0.3-0.125.23794027 • VMware_bootbank_loadesx_7.0.3-0.125.23794027

PRs Fixed	3317204
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

Intel-i40en_1.11.1.32-1vmw.703.0.125.23794027

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_i40en_1.11.1.32-1vmw.703.0.125.23794027
PRs Fixed	3266231
CVE numbers	N/A

Updates the `i40en` VIB to resolve the following issue:

PR 3266231: If the Maximum Segment Size (MSS) in a TCP packet is less than 64 bytes, Intel X700 series NICs might drop network connection

Intel X700 series NICs regard TCP packets with MSS less than 64 bytes as malicious. As a result, Intel X700 series NICs might not process the Tx path when a VM tries to send such packets, which breaks network connectivity.

This issue is resolved in this release. The fix makes sure that the Intel i40en driver automatically corrects the MSS to a valid size.

VMware-NVMeoF-TCP_1.0.0.3-1vmw.703.0.125.23794027

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_nvmetcp_1.0.0.3-1vmw.703.0.125.23794027
PRs Fixed	3297607, 3281791
CVE numbers	N/A

Updates the `nvmetcp` VIB to resolve the following issue:

PR 3297607: An ESXi host might fail with a purple diagnostic screen while connecting to an NVMe over TCP controller

Due to a rare issue in the nvmetcp driver, an ESXi host might fail with a purple diagnostic screen while connecting to an NVMe over TCP controller. In the backtrace, you see a warning such as `WARNING: NVMFDEV:xxxx Failed to connect controller.`

This issue is resolved in this release.

PR 3281791: I/Os might fail on a NVMe over TCP controller with data digest enabled

If the data digest field exceeds a single memory buffer, the nvmetcp driver might not be able to read it. As a result, the driver might drop the NVMe over TCP connection and trigger a queue reset. If this situation repeats, I/O errors start to occur, which might cause issues such as NVMe over TCP storage becoming inaccessible or applications failing, or in the worst case, the ESXi host might fail with a purple diagnostic screen. In the vmkernel logs, you can see an error such as `Failed to receive data digest: Failure.`

This issue is resolved in this release.

VMware-ahci_2.0.11-3vmw.703.0.125.23794027

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_vmw-ahci_2.0.11-3vmw.703.0.125.23794027
PRs Fixed	3284149
CVE numbers	N/A

Updates the `vmw-ahci` VIB to resolve the following issue:

PR 3284149: Messages from the vmw_ahci driver flood the vmkernel log

On some servers, an Advanced Host Controller Interface (AHCI) controller might report an unexpected interrupt signal, Port Connect Change Status, very frequently even if no device is connected. As a result, the vmw_ahci driver sends the following message in the vmkernel log files about 100 times every second:

```
vmw_ahci[000000170]:<0> CompletionBottomHalf:hotplug port status: 40, IPM(0), SPD(0), DET(1)
vmw_ahci[000000170]:<0> CompletionBottomHalf:Port Status Reporting Port Connect Enable: Clearing PxSER-
R.DIAG.x
vmw_ahci[000000170]:<0> CompletionBottomHalf:hotplug port status: 40, IPM(0), SPD(0), DET(0)
vmw_ahci[000000170]:<0> CompletionBottomHalf:Port Status Reporting Port Connect Enable: Clearing PxSERR.DIAG.x
```

This issue is resolved in this release. With the fix, the AHCI controller no longer generates Port Connect Change Status interrupt signals and the driver no longer prints such messages.

ESXi_7.0.3-0.120.23794019

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_crx_7.0.3-0.120.23794019 • VMware_bootbank_cpu-microcode_7.0.3-0.120.23794019 • VMware_bootbank_gc_7.0.3-0.120.23794019 • VMware_bootbank_esx-xserver_7.0.3-0.120.23794019

	• VMware_bootbank_bmcal_7.0.3-0.120.23794019 • VMware_bootbank_vdfs_7.0.3-0.120.23794019 • VMware_bootbank_native-misc-drivers_7.0.3-0.120.23794019 • VMware_bootbank_trx_7.0.3-0.120.23794019 • VMware_bootbank_vsanhealth_7.0.3-0.120.23794019 • VMware_bootbank_esx-base_7.0.3-0.120.23794019 • VMware_bootbank_vsan_7.0.3-0.120.23794019 • VMware_bootbank_esxio-combiner_7.0.3-0.120.23794019 • VMware_bootbank_esx-ui_2.13.2-22721163 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.120.23794019
PRs Fixed	3352357, 3340944, 3330942, 3293531, 3368526, 3373896, 3378149, 3331610, 3293308, 3269602, 3293518, 3312311, 3293459, 3293188, 3260854, 3293307, 3302202, 3293541, 3269861, 3296323, 3280714, 3293185, 3388772
CVE numbers	CVE-2024-22273

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `crx, cpu-microcode, gc, esx-xserver, bmcal, vdfs, native-misc-drivers, trx, vsanhealth, esx-base, vsan, esxio-combiner, esx-ui`, and `esx-dvfilter-generic-fastpath` VIBs to resolve the following issues:

ESXi 7.0 Update 3q provides the following security updates:

- The Python library is updated to version 3.8.18.
- The zlib library is updated to version 1.3.
- The cURL library is updated to version 8.4.0.
- The c-ares C library is updated to version 1.19.1.

ESXi 7.0 Update 3q includes the following Intel microcode:

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x4003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x5003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Cooper Lake	0x5065b (06/55/b)	0xbf	0x7002703	3/21/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0xe000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x38	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0xd0003b9	9/1/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x1000268	9/8/2023	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	0xb4	9/7/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	0x34	9/7/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	0x4e	9/7/2023	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	0x2c000321	8/21/2023	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	0x2b000541	8/21/2023	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0xf4	2/23/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Coffee Lake	0x906ea (06/9e/a)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0xfa	2/27/2023	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x5d	9/3/2023	Intel Xeon E-2300 Series
Raptor Lake E/HX/S	0xb0671 (06/b7/1)	0x32	0x11e	8/31/2023	Intel Xeon E-2400 Series

esx-update_7.0.3-0.120.23794019

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.120.23794019 • VMware_bootbank_esx-update_7.0.3-0.120.23794019
PRs Fixed	N/A
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

VMware-VM-Tools_12.3.5.22544099-23794019

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_locker_tools-light_12.3.5.22544099-23794019
PRs Fixed	3304808
CVE numbers	N/A

Updates the `tools-light` VIB.

VMware Tools Bundling Changes in ESXi 7.0 Update 3q

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3q:

- **windows.iso**: VMware Tools 12.3.5 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
- **linux.iso**: VMware Tools 10.3.26 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- VMware Tools 12.3.5 Release Notes
- Earlier versions of VMware Tools
- What Every vSphere Admin Must Know About VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- Updating VMware Tools

ESXi-7.0U3q-23794027-standard

Profile Name	ESXi-7.0U3q-23794027-standard
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom
Release Date	May 21, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.125.23794027 • VMware_bootbank_esx-xserver_7.0.3-0.125.23794027 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.125.23794027 • VMware_bootbank_esxio-combiner_7.0.3-0.125.23794027 • VMware_bootbank_vdfs_7.0.3-0.125.23794027 • VMware_bootbank_crx_7.0.3-0.125.23794027 • VMware_bootbank_esx-ui_2.13.2-22721163 • VMware_bootbank_esx-base_7.0.3-0.125.23794027 • VMware_bootbank_trx_7.0.3-0.125.23794027 • VMware_bootbank_vsanhealth_7.0.3-0.125.23794027 • VMware_bootbank_cpu-microcode_7.0.3-0.125.23794027 • VMware_bootbank_native-misc-drivers_7.0.3-0.125.23794027 • VMware_bootbank_vsan_7.0.3-0.125.23794027 • VMware_bootbank_bmcal_7.0.3-0.125.23794027 • VMware_bootbank_esx-update_7.0.3-0.125.23794027 • VMware_bootbank_loadesx_7.0.3-0.125.23794027 • VMW_bootbank_i40en_1.11.1.32-1vmw.703.0.125.23794027

	• VMW_bootbank_nvmetcp_1.0.0.3-1vmw.703.0.125.23794027 • VMW_bootbank_vmw-ahci_2.0.11-3vmw.703.0.125.23794027 • VMware_locker_tools-light_12.3.5.22544099-23794019
PRs Fixed	3269229, 3336578, 3332098, 3324772, 3337108, 3319535, 3336916, 3331375, 3326805, 3335978, 3267977, 3323978, 3331256, 3332691, 3313970, 3312843, 3309601, 3317598, 3323119, 3326739, 3317618, 3244429, 3328641, 3328638, 3328337, 3326300, 3329238, 3328301, 3297696, 3296093, 3317448, 3285491, 3276174, 3297629, 3314959, 3309482, 3320147, 3297625, 3297729, 3311303, 3297704, 3309472, 3297749, 3298709, 3320949, 3310432, 3297774, 3302255, 3270210, 3311302, 3257098, 3311831, 3309603, 3317088, 3321157, 2964964, 3305227, 3318350, 3256083, 3269969, 3317445, 3314400, 3267704, 2760003, 3313882, 3243360, 3293469, 3284876, 3265330, 3303842, 3303855, 3293093, 3309148, 3307580, 3301661, 3304469, 3260297, 3260070, 3297409, 3252235, 3287748, 3306033, 3273752, 3288607, 3289238, 3284916, 3303694, 3284133, 3273653, 3298508, 3289605, 3289669, 3291198, 3240347, 3280468, 3285518, 3283501, 3275377, 3267449, 3282267, 3256992, 3251790, 3275137, 3240662, 3259035, 3259205, 3266912, 3282224, 3273653, 3346924, 3346935, 3346816, 3237506, 3331539, 3271089, 3291105, 3346938, 3312150, 3284149, 3266231, 3317204, 3297607, 3281791
Related CVE numbers	CVE-2024-22273

This patch updates the following issues:

PR 3318350: The sfcb service might fail and generate multiple dump files

Due to a NULL reference, the sfcbd service might fail. You see multiple dump core files created at `/var/core/sfcb-vmware_bas-zdump.`.

This issue is resolved in this release.

PR 3284149: Messages from the vmw_ahci driver flood the vmkernel log

On some servers, an Advanced Host Controller Interface (AHCI) controller might report an unexpected interrupt signal, Port Connect Change Status, very frequently even if no device is connected. As a result, the vmw_ahci driver sends the following message in the vmkernel log files about 100 times every second:

```
vmw_ahci[000000170]:<0> CompletionBottomHalf:hotplug port status: 40, IPM(0), SPD(0), DET(1)
vmw_ahci[000000170]:<0> CompletionBottomHalf:Port Status Reporting Port Connect Enable: Clearing PxSER-
R.DIAG.x
vmw_ahci[000000170]:<0> CompletionBottomHalf:hotplug port status: 40, IPM(0), SPD(0), DET(0)
vmw_ahci[000000170]:<0> CompletionBottomHalf:Port Status Reporting Port Connect Enable: Clearing PxSERR.DIAG.x
```

This issue is resolved in this release. With the fix, the AHCI controller no longer generates Port Connect Change Status interrupt signals and the driver no longer prints such messages.

PR 3297607: An ESXi host might fail with a purple diagnostic screen while connecting to an NVMe over TCP controller

Due to a rare issue in the nvmetcp driver, an ESXi host might fail with a purple diagnostic screen while connecting to an NVMe over TCP controller. In the backtrace, you see a warning such as `WARNING: NVMFDEV:xxxx Failed to connect controller.`.

This issue is resolved in this release.

PR 3281791: I/Os might fail on a NVMe over TCP controller with data digest enabled

If the data digest field exceeds a single memory buffer, the nvmetcp driver might not be able to read it. As a result, the driver might drop the NVMe over TCP connection and trigger a queue reset. If this situation repeats, I/O errors start to occur, which might cause issues such as NVMe over TCP storage becoming inaccessible or applications failing, or in the worst case, the ESXi host might fail with a purple diagnostic screen. In the vmkernel logs, you can see an error such as `Failed to receive data digest: Failure.`

This issue is resolved in this release.

PR 3266231: If the Maximum Segment Size (MSS) in a TCP packet is less than 64 bytes, Intel X700 series NICs might drop network connection

Intel X700 series NICs regard TCP packets with MSS less than 64 bytes as malicious. As a result, Intel X700 series NICs might not process the Tx path when a VM tries to send such packets, which breaks network connectivity.

This issue is resolved in this release. The fix makes sure that the Intel i40en driver automatically corrects the MSS to a valid size.

PR 3317598: A disk in a vSAN cluster might fail without an error and cause unresponsiveness or failure of virtual machines in the cluster

In rare cases, if an I/O is stuck due to a hardware of firmware issue on a disk in a vSAN cluster, and a transient error occurs at the same time, a race between the stuck I/O and the transient error handling might cause a deadlock. vSAN does not process any reports on events after the deadlock and you do not receive any notifications. As a result, virtual machines on the cluster of the affected disk become unresponsiveness or fail without logs or warning.

This issue is resolved in this release.

PR 3273653: In vSphere systems using memory cards larger than 64GB, you might see "Unable to allocate SCSI_Command" log messages

If you use physical memory cards larger than 64GB for your vSphere system, whenever the number of VM count increases, you might see errors for the SCSI command slab and heap allocations such as `VSCSI: 590: VSCSI_VmkAccumulateSG failed: Out of memory` or `Unable to allocate SCSI_Command.`

This issue is resolved in this release. The fix applies a scale factor based on the size of the physical memory.

PR 3326739: You do not get debugging logs when the vmkdevmgr service fails

In very rare cases, if the vmkdevmgr service fails and core dumps are not enabled, you might not get debugging logs that help you to identify the underlying issue for the failure.

This issue is resolved in this release. The fix adds an automatic check if core dumps for the vmkdevmgr service are enabled.

PR 3309601: The vSphere Virtual Volumes service might fail with a dump while applying a VM Policy to a VM on an ESXi host

In the rare case when an untracked reference to a vendor provider parameter in a vSphere API for Storage Awareness (VASA) session is accessed after deletion, it might cause dump generation. As a result, the vSphere Virtual Volumes service might fail with a dump while applying a VM Policy to a VM on an ESXi host.

This issue is resolved in this release.

PR 3265330: The VMX service might fail during migration of virtual machines with vSphere Virtual Volumes if the volume closure on the source takes long

In some scenarios, such as virtual machines with vSphere Virtual Volumes and Changed Block Tracking (CBT) or Content Based Read Cache (CBRC) enabled, during storage migration, flushing pending I/Os on volume closure at the source might take long, like 10 sec. If clearing the pending I/Os is not complete by the time the VMX service tries to reach the volumes on the destinations host, the service fails.

This issue is resolved in this release. The fix makes sure that all vSphere Virtual Volumes and disks are closed on the source host before the destination host tries to open them.

PR 3331375: Path to SATA drives might move to permanently lost state during a secure wipe operation

During a secure wipe operation, some SATA drives might not provide proper vital product data (VPD) to queries from the host. As a result, the HPP plug-in might incorrectly interpret changes in the physical media and mark a path for the SATA device as permanently lost.

This issue is resolved in this release.

PR 3328638: An ESXi host might fail with a purple diagnostic screen when probe I/Os fail with a retriable error for a long time

In rare scenarios, if for a long period an adapter or device continues to retry an operation that has failed due to a short-lived disruption such as a transient device error or controller reset, a CPU lockup might occur. As a result, an ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3293469: In the vSphere Client, you see a flat line in the read/write IO latency stats for a vSphere Virtual Volumes datastore

In the vSphere Client, when you navigate to **Monitor >Advanced >Datastore** to see the advanced performance metrics of a virtual machine, you might see a flat line in the read/write I/O latency stats for a vSphere Virtual Volumes datastore. The issue occurs due to incorrect calculation of the counters for the read/write I/O latency as a cumulative average.

This issue is resolved in this release.

PR 3303842: WRITE SAME (16) commands with the unmap bit set fail on thick disks

If information from the VPD Page B2 does not prevent the guest OS from activating the unmap bit in a `WRITE SAME (16)` command on thick disks, the command expectedly fails in a vSphere environment. In addition, if the guest OS does not receive a proper error code, it keeps issuing unmap requests by using `WRITE SAME (16)` , also called block zeroing, and this causes I/O errors.

This issue is resolved in this release. With the fix, VPD Page B2 returns proper reports for `WRITE SAME (16)` with unmap support and the guest OS receives a proper error code when unmap is not supported, to prevent unnecessary unmap attempts by the guest.

PR 3314400: An ESXi host fails with a purple diagnostic screen and message @BlueScreen: NMI IPI: Panic requested by another PCPU

In vSphere environments with NSX Data Center, an additional sanity check of the vmxnet3 driver might cause a port or portset lock that might lead to a lock contention. As a result, an ESXi host might fail with a purple diagnostic screen and message `@BlueScreen: NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release. The fix removes the unnecessary vmxnet3 driver check.

PR 3346924: Upgrade of VMware NSX fails due to a stale DVSPORT_FLAG_RESERVED flag

In very rare cases, a failed vSphere vMotion task might keep a `DVSPORT_FLAG_RESERVED` flag on a port and prevent upgrades of VMware NSX, because the switch on which the port resides cannot be removed. Only a restart of the ESXi host can clean the flag.

This issue is resolved in this release.

PR 3243360: You do not see ESXi host names in the Integrated Dell Remote Access Controller (iDRAC)

When you run the command `localcli hardware ipmi bmc get` in an iDRAC environment, some of the fields for ESXi host names are empty.

This issue is resolved in this release. The fix updates the IPMI BMC hostname during static IP configuration, when the ESXi host is statically configured and rebooted.

PR 3289605: Deactivated transmit queuing option might prevent you from optimizing networking performance

If the `NetSchedHClkVnicMQ` advanced option for transmit queuing is not active, a VNIC with multiple queues might not be able to utilize all queues and prevent significant enhancement of the throughput.

This issue is resolved in this release. The fix makes the `NetSchedHClkVnicMQ` option active by default.

PR 3346935: Migration of virtual machines might fail when vSphere Network I/O Control is active on an ESXi host port to which container ports are mapped to

In rare cases, migrating virtual machines might fail when vSphere Network I/O Control is active on an ESXi host port to which container ports are mapped to, because a dummy port is created at the destination host.

This issue is resolved in this release.

PR 3301661: An I/O filter provider might show offline because of IOFilterVP memory leak

Due to a memory leak in IOFilterVP, an I/O filter provider for an ESXi host might show offline in the vSphere Client under **Configure** > **Storage**. The issue occurs because the SSL cache might consume all heap memory to process VASA API requests.

This issue is resolved in this release. The fix adds a timeout for SSL caching sessions to prevent the memory leak.

PR 3346816: You cannot update the VIB for the NVIDIA GRID vGPU graphics card without rebooting the ESXi host

In case the VIB for the NVIDIA GRID vGPU graphics card is large, lack of sufficient space allocated for the kernel module might prevent automatic update and the operation requires a manual reboot of the ESXi host to complete.

This issue is resolved in this release.

PR 3309482: vSAN host fails with purple diagnostic screen during reboot or mounting a vSAN disk group

A rare issue might cause an incorrect initialization of an internal attribute of a component during recovery of the vSAN logical log, LLOG. As a result, the vSAN host might fail with purple diagnostic screen and in the logs you see an error such as:

```
VMK_ASSERT(cfDisableAssert || LSNEntryLessThan(entry, cfParams->gcpEntry))
```

This issue is resolved in this release.

PR 3306033: You need to manually open the firewall at ports that are different from the default 514 for TCP/UDP and 1514 for SSL protocols

Starting with ESXi 7.0 Update 3q, when you configure syslog remote hosts, or loghosts, with non-standard ports, the vmsyslogd service automatically creates persistent dynamic firewall rules. You no longer need to manually open the firewall at ports that are different from the default 514 for TCP/UDP and 1514 for SSL protocols respectively. When configuring remote hosts with the standard ports, you still need to enable the syslog firewall ruleset.

This issue is resolved in this release. For more information, see Opening the firewall for syslog emission to remote hosts.

PR 3282267: The hostd service might intermittently fail due to an invalid sensor data record

In rare cases, the Baseboard Management Controller (BMC) might provide an invalid sensor data record to the hostd service and cause it to fail. As a result, ESXi hosts become unresponsive or disconnect from vCenter.

This issue is resolved in this release. The fix implements checks to validate the sensor data record before passing it to the hostd service.

PR 3237506: What If analysis on vSAN Capacity screen shows incorrect values when using RAID5 or RAID6 storage policy

In vSAN cluster **Capacity** screen, the What If analysis might show incorrect free space when the cluster is using a RAID5 or RAID6 storage policy.

This issue is resolved in this release.

PR 3276174: vSphere vMotion operations between ESXi 7.x hosts fail with the error "Destination failed to preopen disks"

If on an ESXi 7.x host you use an older Virtual Volumes storage provider, also called a VASA provider, it might not allow binding multiple vSphere Virtual Volumes in batches to optimize the performance of migration and power on. As a result, in the vSphere Client you might see the error `Destination failed to preopen disks` when running vSphere vMotion operations between 7.x hosts.

This issue is resolved in this release.

PR 3311831: ESXi hosts intermittently fail with a purple diagnostic screen and the error "Spin count exceeded - possible deadlock"

Due to a rare issue with packets that might be out of order in a TCP connection, you might see ESXi hosts intermittently to fail with a purple diagnostic screen and the error `Spin count exceeded - possible deadlock`. In the `vmkernel.log` file, you see a backtrace for errors in the tcpip stack such as:

```
2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bbf0:
[0x42003081b976]Lock_CheckSpinCount@vmkernel#nover+0x26f stack: 0xffffffffffffff8,
0x15a8f9ed9da6c33, 0x3ff, 0x43201ac1efd8, 0x1

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bc40:
[0x420030908c8d]SP_WaitReadLock@vmkernel#nover+0xba stack: 0x43201ac1efd8, 0x43201ac1efdc,
0x0, 0x0, 0x41ffd380b7a0

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bc80:
[0x420030908d2a]SPAcqWriteLockWork@vmkernel#nover+0x33 stack: 0x43201ac10f60,
0x420031ce1595, 0x43201cac3b80, 0x420031d4da3b, 0x43201cac3b80

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bca0:
[0x420031ce1594]rw_wlock@(tcpip4)#<None>+0x8d stack: 0x43201cac3b80, 0x41ffd38030b0, 0x6,
0x41ffd380b7a0, 0x43201ac10f60

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bcb0:
[0x420031d4da3a]tcp_usr_attach@(tcpip4)#<None>+0x7b stack: 0x6, 0x41ffd380b7a0,
0x43201ac10f60, 0x43201ac1aff0, 0x453c10e1bd58

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bcf0:
[0x420031cff0a6]socreate@(tcpip4)#<None>+0x1fb stack: 0x58, 0x43201ac1aff0,
0x41ffd380b7a0, 0x1, 0x6

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bd40:
[0x420031ceb2b6]vmk_socket@(tcpip4)#<None>+0xa3 stack: 0x1, 0x420031ccf047,
0x45dbc1758950, 0x4313d2803210, 0x43201ac01700
```

This issue is resolved in this release.

PR 3252235: ESXi hosts might fail to boot due to a rare deadlock between open and rename operations on objects with parent-child relationship

A rename operation locks the source and destination directories based on the object pointer address with the assumption that the parent object has the lower address. In rare cases, the assumption might not be correct and the rename lock can happen for the child first and then the parent, while the open operation locks the parent first and then the child. As a result, a deadlock between the open and rename operations occurs and ESXi hosts fail to boot.

This issue is resolved in this release.

PR 3313970: ESXi hosts might fail with a purple diagnostic screen due to a write lock of the uplink watchdog

During a regular sanity check, the uplink watchdog might hold a write lock that prevents reads from other services and might cause the ESXi host might fail with a purple diagnostic screen. In the backtrace, you see errors such as:

```
Panic Message: @BlueScreen: NMI IPI: Panic requested by another PCPU. RIPOFF(base):RBP:CS
[0x14e1e0(0x420033000000):0x430201d03440:0xf48] (Src 0x4, CPU14).
```

This issue is resolved in this release. The fix replaces the write lock with a read lock for regular sanity checks.

PR 3331539: Migration between NSX segments with many container logical ports might cause an ESXi host to fail with a purple diagnostic screen

A rare race condition between vSphere vMotion tasks on NSX Segments with many container logical ports might cause an ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3240662: Host Profile compliance check throws incorrect error message "IPv4 vmknic gateway configuration doesn't match the specification"

In the vSphere Client, you might see the error `IPv4 vmknic gateway configuration doesn't match the specification` when running a compliance check on a Host Profile. The error remains even when you remediate the Host Profile. However, the default gateway settings are defined from the Host Customization workflows and you should not see such an error message during compliance checks. Disregard the message, as it does not affect the host profile functions.

This issue is resolved in this release.

PR 3271089: Virtual machines with a lightweight delta (LWD) snapshot might fail to start after a failure of the vmx service

In rare cases, if the vmx service fails during the creation of a LWD snapshot, some partially initialized LWD snapshot files might remain on the datastore. As a result, virtual machines with such LWD snapshots might fail to start due to validation failures.

This issue is resolved in this release.

PR 3304469: vSphere vMotion operations might fail due to a rare issue with no namespaces present in the namespacemgr.db file

When a virtual machine is configured with namespaces and for some reason the namespaces table in the `namespacemgr.db` file is empty in the ESXi host database, migration of such a VM by using vSphere vMotion might fail. In the `vmware.log` file, you see errors such as:

```
vmx - NamespaceMgrCheckpoint: No valid queue found while restoring the namespace events.
The migrate type is 1.
```

This issue is resolved in this release.

PR 3291105: While detaching an Enhanced Networking Stack (ENS) port from an ESXi host, the host might fail with a purple diagnostic screen

During deactivation of ENS in scenarios such as an upgrade or a VNIC configuration change, while detaching an ENS port from an ESXi host with active ENS, the port might be removed from the port list and not be available for further reference, which might cause an invalid memory access error. As a result, the ESXi host fails with a purple diagnostic screen.

This issue is resolved in this release.

PR 3346938: After a NSX Distributed Security installation, vSphere vMotion might not restore a switch security filter on the destination side

When you opt to install the Security Only option of NSX Distributed Security, vSphere vMotion might not restore a switch security filter on the destination side and the Address Resolution Protocol (ARP) fails.

This issue is resolved in this release.

PR 3312150: Failover of VMs on vSphere Virtual Volume datastores might fail due to wrong order of metadata from vSphere API for Storage Awareness (VASA) provider

Certain VASA providers might return metadata info in a different order than what an ESXi host requests. As a result, when VMs on a vSphere Virtual Volume datastore fail over to a recovery site, the VMs cannot reboot on the target site.

This issue is resolved in this release. With the fix, even if a VASA provider returns metadata info in a different order from the ESXi host request, failover succeeds.

PR 3328641: An ESXi host might fail with a purple diagnostic screen due to a rare issue during a read-modify-write (RMW) operation

On 512e software emulated devices, when I/O requests are not multiple of 4096, ESXi runs RMW operations. In such cases, the final write I/O issue path can access the write command frame after the write is issued to the target. If the target completes the write request before the issue path accesses the write frame, the write frame is freed. As a result, you might see a Use-After-Free scenario that might lead to failure of the ESXi host with a purple diagnostic screen.

This issue is resolved in this release.

PR 3332098: Asynchronous write operations to a SMB file share on the vSAN File Service might cause data transfer issues

In rare cases, a race condition during asynchronous write operations to a SMB file share on the vSAN File Service might cause data transfer issues such as truncation.

This issue is resolved in this release.

PR 3256992: vSphere vMotion tasks fail for VMs on port groups with promiscuous mode enabled

A rare issue with corrupted network packets that becomes evident in secure network protocols, where packet data integrity is checked upon receipt, might lead to connectivity issues on port groups with promiscuous mode enabled. As a result, you might see vSphere vMotion tasks failing for VMs on such port groups. You see data integrity errors such as `Failed to decrypt ciphertext` in the backtrace.

This issue is resolved in this release.

PR 3244429: Exit Code 127 error in the hostd service might cause an ESXi host to disconnect temporarily from vCenter

Due to an issue in the open source glibc components, attempts by hostd to process the list of installed I/O filters on an ESXi host might intermittently cause an Exit Code 127 error. In the `/var/run/log/syslog.log` , you see lines such as:

```
2022-10-13T08:00:20.180Z watchdog-hostd[<PID>]: 'hostd ++min=0,swapscope=system' exited after X seconds 127
```

As a result, the ESXi host temporarily disconnects from vCenter until the hostd watchdog restarts the service and connectivity restores. The issue has been observed while loading the `vmwarelwd` I/O filter.

This issue is resolved in this release. ESXi 7.0 Update 3q adds a hostd configuration option that allows you to deactivate an I/O filter without removing it from the vCenter system and skip reporting such filters in the host configuration overhead. To use the option, log in to SSH and complete the following steps:

1. Set the `plugins/hostsvc/report_disabled_filters_in_host_config` option in the hostd configuration to `False` as described in VMware knowledge base article 82227.

2. Deactivate the `vmwarelwd` filter by running the following python script directly on the host:

```
import vmware.vsi as vsi
vsi.set('/iofilters/statusDisabledEvent', {'filterName': 'vmwarelwd', 'failureReason' :
'workaround'})
```

PR 3332691: vSAN IOPS performance data not available for VM multi-writer virtual disk

The following performance charts for a vSAN VM multi-writer virtual disk, under **Monitor** > **vSAN** > **Performance** > **Virtual Disks**, are not available: IOPS, IOPS limit, and Delayed Normalized IOPS. These charts are available only for disks without active multi-writer mode.

This issue is resolved in this release.

PR 3288607: An ESXi host might fail with a purple diagnostic screen due to a rare storage heap corruption in NVMe devices

In rare cases, an I/O thread from a NVMe device, such as deleting a virtual machine from a datastore using NVMe devices, might complete before the High-Performance Plug-in (HPP) claims the device to complete the thread. As a result, HPP tries to access a non-existing thread which leads to a failure of the ESXi host with a purple diagnostic screen and an error such as `PSOD @BlueScreen: PANIC bora/vmkernel/main/dlmalloc.c:4763`.

This issue is resolved in this release.

PR 3273752: ESXi hosts fail with a purple diagnostic screen and a #PF Exception 14 in world 2097479:HELPER_SCSI_ error

After a change in the namespace list for a controller, for example the PsaNvmeController, the update semaphore works as expected, but the change might not complete because no lock is available. As a result, the ESXi host fails with a purple diagnostic screen and a `#PF Exception 14 in world 2097479:HELPER_SCSI_ error`.

This issue is resolved in this release.

PR 3267977: You might see spikes in the latency performance metrics after creating a virtual machine disk snapshot

After you create a virtual machine disk snapshot, you might see latency spikes in the vSphere performance charts. Such unusual spikes are due to the recreation of some internal system objects and the restart of the latency performance counters in the storage subsystem.

This issue is resolved in this release. The fix prevents false latency alarms after taking virtual machine disk snapshots.

PR 3305227: If you do not increase the TCP/IP heap memory limit before installation of NSX-T Data Center kernel modules, ESXi hosts might crash

When you install NSX-T Data Center kernel modules on ESXi hosts with high loads, the pre-allocated TCP/IP heap during boot required for the operation might not be sufficient and cause the ESXi host to fail with a purple diagnostic screen. The issue occurs when the TCP/IP heap cannot grow quickly enough to provide a continuous allocation of 2 MB of memory in case of memory fragmentation on such ESXi hosts. As a result, ESXi hosts might fail with a purple diagnostic screen and a `vmkernel.log` error such as

```
Heap: 3707: Heap tcpip (44384680/1073746344): Maximum allowed growth (1048576) too small
for size (1203496)
```

The purple diagnostic screen failure is less likely to occur if you put the ESXi host in maintenance mode before the NSX-T Data Center kernel modules installation, as MM significantly reduces the memory pressure.

This issue is partially resolved in this release. Starting from ESXi 7.0 Update 3, if you are planning an NSX-T Data Center installation, you can increase the `TcpipHeapSize` limit pre-allocated during boot to 128 MB. For example, if you want to increase the `TcpipHeapSize` allocation to the maximum, you can use the following steps:

1. Increase the heap size to 128 MB by using the command `esxcfg-advcfg -s 128 /Net/TcpipHeapSize`

2. Confirm that the heap size is 128 MB: `esxcfg-advcfg -g /Net/TcpipHeapSize`
3. Reboot the ESXi host.

To avoid this issue, you can reboot the ESXi host and install NSX-T Data Center with no VMs running.

PR 3328301: ESXi hosts might fail with a purple diagnostic screen due to a race condition in the High Performance Plug-in (HPP)

Due to a rare race condition in HPP, when a storage path failover and device deletion occur at the same time, ESXi hosts might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3257098: A virtual machine fails with McastFilter_Deactivate error

In very rare cases, when a VM is low on memory, a code path might not initialize all its members on restart and cause the VM to fail with a purple diagnostic screen and an error such as `McastFilter_Deactivate`.

This issue is resolved in this release. Avoid low memory state of VMs to prevent similar issues.

PR 3317448: IPv6 routing disappears after you deactivate router advertisement on an ESXi host and the host loses connectivity

Deactivating IPv6 router advertisements (RA) on the physical network or deselecting the option "Obtain IP Address through Router Advertisement" at the VMkernel level might cause the default route for the VMkernel adapter to disappear, even when you have a static IPv6 address on the adapter. The issue occurs only when the IPv6 prefix of both the static IP address and the prefix specified in the RA message are the same. As a result, ESXi incorrectly removes the route entry for that particular subnet, despite that the static IP address is still active for the same prefix, and the ESXi host loses connectivity.

This issue is resolved in this release. Avoid using the same IPv6 prefix for both a static IP address and addresses that are automatically configured in RA messages to prevent the issue.

PR 3312843: ESXi hosts intermittently disconnect from the vCenter system and the hostd service restarts

If an ESXi host uses only one of the multipath plug-ins, either HPP or NMP, when the hostd service collects telemetry data on scheduled intervals, the call might return a null pointer value. Dereferencing the `nullptr` might lead to a hostd failure, but the service automatically restarts. As a result, you see the ESXi host intermittently disconnected from the vCenter system.

This issue is resolved in this release. The fix adds a `nullptr` check.

PR 3328337: The hostd service might become unresponsive after a restart due to a rare issue with Inter Process Communication (IPC)

If an IPC process has incorrect payload in the IPC packet, for example: an incorrect version in the header, a deadlock in the iSCSI daemon might cause the hostd service to become unresponsive after a hostd restart. As a result, you cannot perform any operations on the affected ESXi host and VMs by using the vSphere Client.

This issue is resolved in this release.

PR 3285491: You cannot use host profiles to configure a path selection policy for disks using Raw Device Mapping

In some cases, when you try to change or configure the path selection policy of multiple virtual machines by using a host profile, the operation fails for VMs using Raw Device Mapping.

This issue is resolved in this release.

PR 3296093:ESXi hosts intermittently fail with a purple diagnostic screen and a PF Exception 14 error

While running an ESXi upgrade, a rare race condition in the device registration during disk initialization might lead to an ESXi host failing with a purple diagnostic screen. In the screen, you see an error such as `@BlueScreen: #PF`

`Exception 14 in world XXXXX:HELPER_SCSI_ IP` and in the backtrace, you see `vmk_ScsiGetDeviceState` and `nmp_DeviceUpdatePathStates`.

This issue is resolved in this release.

PR 3321157: You might see network outages in vSphere systems using Intel i40en physical NICs and with Enhanced data path enabled

On Intel i40en NICs, TSO packets that exceed the Maximum Segment Size (MSS) of 8 segments might cause the NIC to become unresponsive. In rare cases, a TSO packet from a VM or from a vmknic might exceed the 8-segement limit and you might see network outages due to blocked pNIC tx traffic. The issue is more likely to occur in vSphere systems using Intel i40en physical NICs and with Enhanced data path enabled.

This issue is resolved in this release.

PR 3307580: Large TCP segmentation offload (TSO) packets might cause network traffic latency and intermittent loss of connectivity for some virtual machines

Environments with the enhanced data path networking stack mode enabled might see network traffic latency and intermittent loss of connectivity for some virtual machines due to an issue with the handling of large TSO packets.

This issue is resolved in this release.

PR 3275137: Rare data corruption issue in vSphere systems that use service insertion might lead to ESXi host failure

In vSphere systems that use service insertion, an error with the check of the available buffer size before pulling data might lead to data corruption that might cause the ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release. The fix makes sure that data pull during service insertion runs only if a sufficient buffer exists.

PR 3270210: The Busybox shell on an ESXi host might fail after you disable echo mode

If you enter a command after `stty -echo`, which disables the echo mode on a Busybox sh shell on an ESXi host, the shell might fail with a coredump.

This issue is resolved in this release.

PR 3319535: Virtual machines with independent_nonpersistent disks might become inaccessible after a VM reset

During a reset, a virtual machine with independent_nonpersistent disks deletes existing redo log files and creates a new redo log. The vmx process updates the new .redo settings in-memory, not in the .vmx file, and when the hostd service reads the disk properties from the .vmx file during sync up, it might consider the redo logs inconsistent. As a result, hostd marks the VM as invalid and the VM becomes inaccessible.

This issue is resolved in this release.

PR 3317445: Enhanced Network Datapath (EDP) might reserve too much memory on a large vSphere system and cause resource issues

EDP reservation is linear to the total memory by reserving up to 1.6% of the total. For a VM with high memory reservation in a large vSphere system, such a memory buffer might be too big. For example, if the system has a 100TB of memory, the EDP reservation might be 1.6TB. As a result, you might see resource issues such as not being able to hot-add VNICs to VMs with high memory reservation.

This issue is resolved in this release. The fix sets the EDP reservation limit at 1% of the total memory and puts a 5GB cap on a single memory reservation. You can adjust the memory reservation limit by using the VMKernel boot option `ensMbufPoolMaxMinMB` or by using the following command: `esxcli system settings kernel set -s ensMbufPoolMaxMBPerGB -v <value-in-MB>`. In any case, you must reboot the ESXi host to enable the change.

PR 3283501: SFCB start, stop, and reporting operations fail due to a stale lockfile: /var/run/sfcbd-init.lock

In rare cases, the `sfcbd-init` script, which creates a lockfile `/var/run/sfcbd-init.lock` to prevent multiple instances of the script from running at the same time, receives a SIGPIPE signal, which terminates the script and leaves the lockfile unhandled. As a result, any further attempts to run the script fail because they cannot acquire the lock.

This issue is resolved in this release. The fix adds SIGPIPE to the list of signals handled by the trap command in the `sfcbd-init` script. This ensures that the lock file is cleared even when the script receives a SIGPIPE signal.

PR 3285243: If an NFS server sends a file handle with 0 length during a new directory creation, ESXi hosts might fail with a purple diagnostic screen

On volumes mounted by using NFSv4.1, if the NFS server sends a file handle with length of 0 in response to a new directory request, the ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3317088: You see slow response times in vSphere environments with NVMe SSDs

When a NVMe SSD fails, it does not respond to any commands from the NVMe driver, such as closing outstanding I/Os. As a result, many I/O and NVMe driver commands might remain pending and cause slow response times in the vSphere environment or even failure of upper layer applications.

This issue is resolved in this release. With the fix, the NVMe driver initiates controller or queue reset in case driver commands are not effective, to allow closing of outstanding I/Os.

PR 3302202: You might see placeholders listed in the Guest OS version drop-down menu for new ESXi virtual machines

When creating a new virtual machine, in the **Guest OS version** drop-down menu you might see placeholders such as Windows 12 and Windows Server 2025. You cannot use such placeholders to create new virtual machines.

This issue is resolved in this release.

PR 3289669: You cannot power on a virtual machine after a failed or canceled export of an Open Virtual Format (OVF) file

A rare deadlock caused by a failed or canceled export of a VM as an OVF file might prevent subsequent start of that VM. The VM appears in a **VM_STATE_EXPORTING** state.

This issue is resolved in this release. If the export of an OVF file fails due to a network outage, you cannot prevent the issue, but you can avoid it if you do not manually cancel OVF exports. If you already face the issue, restart the hostd service on the affected ESXi host by either using the SSH command `/etc/init.d/hostd restart` or selecting **Restart Management Agents** under **Troubleshooting options** in the Direct Console User Interface. The restart of the host service stops any operations on the ESXi host.

PR 3313882: Virtual machines and data objects might become inaccessible after an ESXi firewall refresh

In some scenarios, a refresh of the ESXi firewall on vSAN clusters might refer to an incomplete object in the ESXi Configuration Store (ConfigStore) and cause the Reliable Datagram Transport (RDT) and Cluster Monitoring, Membership and Directory Service (CMMDS) firewall rules to be disabled. As a result, some clusters might be isolated and virtual machines and data objects might become inaccessible.

This issue is resolved in this release.

PR 3280714: In the web console of Linux virtual machines, the Caps Lock option does not work consistently

When you enable the Caps Lock option in the web console of a Linux virtual machine, the typing output might not consistently be capital letters.

This issue is resolved in this release.

PR 3287440: ESXi hosts stop responding to tasks from the vSphere Client

Due to a rare race condition with accessing vSphere Distributed Switch data from competing services, ESXi hosts might stop responding to tasks from the vSphere Client. For example, in NSX Data Center for vSphere environments, you might see an error such as `TN Profile attachment to the cluster is in progress` that prevents you from running other tasks.

This issue is resolved in this release.

PR 3282224: VXLAN traffic generated from a guest VM to port 4789 fails

ESXi hosts have VXLAN port 8472 enabled by default and not the UDP port 4789, which is the default for NSX 6.2.3 and later. As a result, traffic to VXLAN port 4789 fails.

This issue is resolved in this release. The fix adds port 4789 to the list of VXLAN ports by default.

PR 3260070: ESXi hosts might fail with a purple diagnostic screen due to a NULL pointer reference in a tardisk object

A NULL pointer violation with `VisorFSTarDoIOInt()` in the backtrace might cause ESXi hosts to fail with a purple diagnostic screen. The issue occurs in the following conditions:

1. A vSphere admin manually logs into the host by using SSH
2. Modifies a tardisk file, for example in `/etc` , without re-writing the file completely
3. Performs an upgrade that replaces a VIB containing that specific file
4. The admin or an ESXi service access the modified file

This issue is resolved in this release.

PR 3284133: ESXi hosts in environments with NVMe PCIe devices might temporarily lose connectivity during collection of diagnostic information

When you use the `vm-support` command to collect information about ESXi systems such as network, storage, and vSAN, logs for the telemetry and persistent events of NVMe PCIe controllers are temporally stored in the ramdisk `/tmp` directory. If your system has many NVMe PCIe devices or the log file is large, the ramdisk `/tmp` directory quickly becomes full. As a result, ESXi hosts in environments with NVMe PCIe devices might temporarily lose connectivity until the `vm-support` collection completes.

This issue is resolved in this release. The fix selects the VMFS datastore with the most free space to store `nvme` logs and compresses each log file to save storage space.

PR 3275377: VBS-enabled Windows VMs might intermittently fail with a blue diagnostic screen on ESXi hosts running on AMD processors

Windows virtual machines with virtualization-based security (VBS) enabled might intermittently fail with a blue diagnostic screen on ESXi hosts running on AMD processors. The BSOD has the following signature:

```
SECURE_KERNEL_ERROR (18b)The secure kernel has encountered a fatal error.
Arguments:
Arg1: 000000000000018c
Arg2: 000000000000100b
Arg3: 0000000000000000
Arg4: 000000000000409b
```

This issue is resolved in this release.

PR 3259205: A stateless ESXi host might lose connection to vCenter after a reboot

During the boot of a stateless ESXi host, in very rare situations, the management vmknic might change unexpectedly and change the IP address of the host. As a result, the host disconnects from vCenter. If you apply a host profile, in the vSphere Client you might see an error such as **Host profile apply failed with error: Error: A specified parameter was not correct: SelectVnic.vnic.Specification.NetStackInstanceKey.**

This issue is resolved in this release.

ESXi-7.0U3q-23794027-no-tools

Profile Name	ESXi-7.0U3q-23794027-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom
Release Date	May 21, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.125.23794027 • VMware_bootbank_esx-xserver_7.0.3-0.125.23794027 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.125.23794027 • VMware_bootbank_esxio-combiner_7.0.3-0.125.23794027 • VMware_bootbank_vdfs_7.0.3-0.125.23794027 • VMware_bootbank_crx_7.0.3-0.125.23794027 • VMware_bootbank_esx-ui_2.13.2-22721163 • VMware_bootbank_esx-base_7.0.3-0.125.23794027 • VMware_bootbank_trx_7.0.3-0.125.23794027 • VMware_bootbank_vsanhealth_7.0.3-0.125.23794027 • VMware_bootbank_cpu-microcode_7.0.3-0.125.23794027 • VMware_bootbank_native-misc-drivers_7.0.3-0.125.23794027 • VMware_bootbank_vsan_7.0.3-0.125.23794027 • VMware_bootbank_bmcal_7.0.3-0.125.23794027 • VMware_bootbank_esx-update_7.0.3-0.125.23794027 • VMware_bootbank_loadesx_7.0.3-0.125.23794027 • VMW_bootbank_i40en_1.11.1.32-1vmw.703.0.125.23794027 • VMW_bootbank_nvmetcp_1.0.0.3-1vmw.703.0.125.23794027 • VMW_bootbank_vmw-ahci_2.0.11-3vmw.703.0.125.23794027
PRs Fixed	3269229, 3336578, 3332098, 3324772, 3337108, 3319535, 3336916, 3331375, 3326805, 3335978, 3267977, 3323978, 3331256, 3332691, 3313970, 3312843, 3309601, 3317598, 3323119, 3326739, 3317618, 3244429, 3328641, 3328638, 3328337, 3326300, 3329238, 3328301, 3297696, 3296093, 3317448, 3285491, 3276174, 3297629, 3314959, 3309482, 3320147, 3297625, 3297729, 3311303, 3297704, 3309472, 3297749, 3298709, 3320949, 3310432, 3297774, 3302255, 3270210, 3311302, 3257098, 3311831, 3309603, 3317088, 3321157, 2964964, 3305227, 3318350, 3256083, 3269969, 3317445, 3314400, 3267704, 2760003, 3313882, 3243360, 3293469, 3284876, 3265330, 3303842, 3303855, 3293093, 3309148, 3307580, 3301661, 3304469, 3260297, 3260070, 3297409, 3252235, 3287748, 3306033, 3273752, 3288607, 3289238, 3284916, 3303694, 3284133, 3273653, 3298508, 3289605, 3289669, 3291198, 3240347, 3280468, 3285518, 3283501, 3275377, 3267449, 3282267, 3256992, 3251790, 3275137, 3240662, 3259035, 3259205, 3266912, 3282224, 3273653, 3346924, 3346935, 3346816, 3237506, 3331539, 3271089, 3291105, 3346938, 3312150, 3284149, 3266231, 3317204, 3297607, 3281791
Related CVE numbers	CVE-2024-22273

This patch updates the following issues:

PR 3318350: The sfcb service might fail and generate multiple dump files

Due to a NULL reference, the sfcbd service might fail. You see multiple dump core files created at `/var/core/sfcb-vmware_bas-zdump.`.

This issue is resolved in this release.

PR 3284149: Messages from the vmw_ahci driver flood the vmkernel log

On some servers, an Advanced Host Controller Interface (AHCI) controller might report an unexpected interrupt signal, Port Connect Change Status, very frequently even if no device is connected. As a result, the vmw_ahci driver sends the following message in the vmkernel log files about 100 times every second:

```
vmw_ahci[000000170]:<0> CompletionBottomHalf:hotplug port status: 40, IPM(0), SPD(0), DET(1)
vmw_ahci[000000170]:<0> CompletionBottomHalf:Port Status Reporting Port Connect Enable: Clearing PxSER-
R.DIAG.x
vmw_ahci[000000170]:<0> CompletionBottomHalf:hotplug port status: 40, IPM(0), SPD(0), DET(0)
vmw_ahci[000000170]:<0> CompletionBottomHalf:Port Status Reporting Port Connect Enable: Clearing PxSERR.DIAG.x
```

This issue is resolved in this release. With the fix, the AHCI controller no longer generates Port Connect Change Status interrupt signals and the driver no longer prints such messages.

PR 3297607: An ESXi host might fail with a purple diagnostic screen while connecting to an NVMe over TCP controller

Due to a rare issue in the nvmetcp driver, an ESXi host might fail with a purple diagnostic screen while connecting to an NVMe over TCP controller. In the backtrace, you see a warning such as `WARNING: NVMFDEV:xxxx Failed to connect controller.`.

This issue is resolved in this release.

PR 3281791: I/Os might fail on a NVMe over TCP controller with data digest enabled

If the data digest field exceeds a single memory buffer, the nvmetcp driver might not be able to read it. As a result, the driver might drop the NVMe over TCP connection and trigger a queue reset. If this situation repeats, I/O errors start to occur, which might cause issues such as NVMe over TCP storage becoming inaccessible or applications failing, or in the worst case, the ESXi host might fail with a purple diagnostic screen. In the vmkernel logs, you can see an error such as `Failed to receive data digest: Failure.`.

This issue is resolved in this release.

PR 3266231: If the Maximum Segment Size (MSS) in a TCP packet is less than 64 bytes, Intel X700 series NICs might drop network connection

Intel X700 series NICs regard TCP packets with MSS less than 64 bytes as malicious. As a result, Intel X700 series NICs might not process the Tx path when a VM tries to send such packets, which breaks network connectivity.

This issue is resolved in this release. The fix makes sure that the Intel i40en driver automatically corrects the MSS to a valid size.

PR 3317598: A disk in a vSAN cluster might fail without an error and cause unresponsiveness or failure of virtual machines in the cluster

In rare cases, if an I/O is stuck due to a hardware of firmware issue on a disk in a vSAN cluster, and a transient error occurs at the same time, a race between the stuck I/O and the transient error handling might cause a deadlock. vSAN does not process any reports on events after the deadlock and you do not receive any notifications. As a result, virtual machines on the cluster of the affected disk become unresponsiveness or fail without logs or warning.

This issue is resolved in this release.

PR 3273653: In vSphere systems using memory cards larger than 64GB, you might see "Unable to allocate SCSI_Command" log messages

If you use physical memory cards larger than 64GB for your vSphere system, whenever the number of VM count increases, you might see errors for the SCSI command slab and heap allocations such as `VSCSI: 590: VSCSI_VmkAccumulateSG failed: Out of memory` or `Unable to allocate SCSI_Command.`

This issue is resolved in this release. The fix applies a scale factor based on the size of the physical memory.

PR 3326739: You do not get debugging logs when the vmkdevmgr service fails

In very rare cases, if the vmkdevmgr service fails and core dumps are not enabled, you might not get debugging logs that help you to identify the underlying issue for the failure.

This issue is resolved in this release. The fix adds an automatic check if core dumps for the vmkdevmgr service are enabled.

PR 3309601: The vSphere Virtual Volumes service might fail with a dump while applying a VM Policy to a VM on an ESXi host

In the rare case when an untracked reference to a vendor provider parameter in a vSphere API for Storage Awareness (VASA) session is accessed after deletion, it might cause dump generation. As a result, the vSphere Virtual Volumes service might fail with a dump while applying a VM Policy to a VM on an ESXi host.

This issue is resolved in this release.

PR 3265330: The VMX service might fail during migration of virtual machines with vSphere Virtual Volumes if the volume closure on the source takes long

In some scenarios, such as virtual machines with vSphere Virtual Volumes and Changed Block Tracking (CBT) or Content Based Read Cache (CBRC) enabled, during storage migration, flushing pending I/Os on volume closure at the source might take long, like 10 sec. If clearing the pending I/Os is not complete by the time the VMX service tries to reach the volumes on the destinations host, the service fails.

This issue is resolved in this release. The fix makes sure that all vSphere Virtual Volumes and disks are closed on the source host before the destination host tries to open them.

PR 3331375: Path to SATA drives might move to permanently lost state during a secure wipe operation

During a secure wipe operation, some SATA drives might not provide proper vital product data (VPD) to queries from the host. As a result, the HPP plug-in might incorrectly interpret changes in the physical media and mark a path for the SATA device as permanently lost.

This issue is resolved in this release.

PR 3328638: An ESXi host might fail with a purple diagnostic screen when probe I/Os fail with a retriable error for a long time

In rare scenarios, if for a long period an adapter or device continues to retry an operation that has failed due to a short-lived disruption such as a transient device error or controller reset, a CPU lockup might occur. As a result, an ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3293469: In the vSphere Client, you see a flat line in the read/write IO latency stats for a vSphere Virtual Volumes datastore

In the vSphere Client, when you navigate to **Monitor >Advanced >Datastore** to see the advanced performance metrics of a virtual machine, you might see a flat line in the read/write I/O latency stats for a vSphere Virtual Volumes datastore. The issue occurs due to incorrect calculation of the counters for the read/write I/O latency as a cumulative average.

This issue is resolved in this release.

PR 3303842: WRITE SAME (16) commands with the unmap bit set fail on thick disks

If information from the VPD Page B2 does not prevent the guest OS from activating the unmap bit in a `WRITE SAME (16)` command on thick disks, the command expectedly fails in a vSphere environment. In addition, if the guest OS does not receive a proper error code, it keeps issuing unmap requests by using `WRITE SAME (16)` , also called block zeroing, and this causes I/O errors.

This issue is resolved in this release. With the fix, VPD Page B2 returns proper reports for `WRITE SAME (16)` with unmap support and the guest OS receives a proper error code when unmap is not supported, to prevent unnecessary unmap attempts by the guest.

PR 3314400: An ESXi host fails with a purple diagnostic screen and message @BlueScreen: NMI IPI: Panic requested by another PCPU

In vSphere environments with NSX Data Center, an additional sanity check of the vmxnet3 driver might cause a port or portset lock that might lead to a lock contention. As a result, an ESXi host might fail with a purple diagnostic screen and message `@BlueScreen: NMI IPI: Panic requested by another PCPU.`

This issue is resolved in this release. The fix removes the unnecessary vmxnet3 driver check.

PR 3346924: Upgrade of VMware NSX fails due to a stale DVSPORT_FLAG_RESERVED flag

In very rare cases, a failed vSphere vMotion task might keep a `DVSPORT_FLAG_RESERVED` flag on a port and prevent upgrades of VMware NSX, because the switch on which the port resides cannot be removed. Only a restart of the ESXi host can clean the flag.

This issue is resolved in this release.

PR 3243360: You do not see ESXi host names in the Integrated Dell Remote Access Controller (iDRAC)

When you run the command `localcli hardware ipmi bmc get` in an iDRAC environment, some of the fields for ESXi host names are empty.

This issue is resolved in this release. The fix updates the IPMI BMC hostname during static IP configuration, when the ESXi host is statically configured and rebooted.

PR 3289605: Deactivated transmit queuing option might prevent you from optimizing networking performance

If the `NetSchedHClkVnicMQ` advanced option for transmit queuing is not active, a VNIC with multiple queues might not be able to utilize all queues and prevent significant enhancement of the throughput.

This issue is resolved in this release. The fix makes the `NetSchedHClkVnicMQ` option active by default.

PR 3346935: Migration of virtual machines might fail when vSphere Network I/O Control is active on an ESXi host port to which container ports are mapped to

In rare cases, migrating virtual machines might fail when vSphere Network I/O Control is active on an ESXi host port to which container ports are mapped to, because a dummy port is created at the destination host.

This issue is resolved in this release.

PR 3301661: An I/O filter provider might show offline because of IOFilterVP memory leak

Due to a memory leak in IOFilterVP, an I/O filter provider for an ESXi host might show offline in the vSphere Client under **Configure** > **Storage**. The issue occurs because the SSL cache might consume all heap memory to process VASA API requests.

This issue is resolved in this release. The fix adds a timeout for SSL caching sessions to prevent the memory leak.

PR 3346816: You cannot update the VIB for the NVIDIA GRID vGPU graphics card without rebooting the ESXi host

In case the VIB for the NVIDIA GRID vGPU graphics card is large, lack of sufficient space allocated for the kernel module might prevent automatic update and the operation requires a manual reboot of the ESXi host to complete.

This issue is resolved in this release.

PR 3309482: vSAN host fails with purple diagnostic screen during reboot or mounting a vSAN disk group

A rare issue might cause an incorrect initialization of an internal attribute of a component during recovery of the vSAN logical log, LLOG. As a result, the vSAN host might fail with purple diagnostic screen and in the logs you see an error such as:

```
VMK_ASSERT(cfDisableAssert || LSNEntryLessThan(entry, cfParams->gcpEntry))
```

This issue is resolved in this release.

PR 3306033: You need to manually open the firewall at ports that are different from the default 514 for TCP/UDP and 1514 for SSL protocols

Starting with ESXi 7.0 Update 3q, when you configure syslog remote hosts, or loghosts, with non-standard ports, the vmsyslogd service automatically creates persistent dynamic firewall rules. You no longer need to manually open the firewall at ports that are different from the default 514 for TCP/UDP and 1514 for SSL protocols respectively. When configuring remote hosts with the standard ports, you still need to enable the syslog firewall ruleset.

This issue is resolved in this release. For more information, see Opening the firewall for syslog emission to remote hosts.

PR 3282267: The hostd service might intermittently fail due to an invalid sensor data record

In rare cases, the Baseboard Management Controller (BMC) might provide an invalid sensor data record to the hostd service and cause it to fail. As a result, ESXi hosts become unresponsive or disconnect from vCenter.

This issue is resolved in this release. The fix implements checks to validate the sensor data record before passing it to the hostd service.

PR 3237506: What If analysis on vSAN Capacity screen shows incorrect values when using RAID5 or RAID6 storage policy

In vSAN cluster **Capacity** screen, the What If analysis might show incorrect free space when the cluster is using a RAID5 or RAID6 storage policy.

This issue is resolved in this release.

PR 3276174: vSphere vMotion operations between ESXi 7.x hosts fail with the error "Destination failed to preopen disks"

If on an ESXi 7.x host you use an older Virtual Volumes storage provider, also called a VASA provider, it might not allow binding multiple vSphere Virtual Volumes in batches to optimize the performance of migration and power on. As a result, in the vSphere Client you might see the error `Destination failed to preopen disks` when running vSphere vMotion operations between 7.x hosts.

This issue is resolved in this release.

PR 3311831: ESXi hosts intermittently fail with a purple diagnostic screen and the error "Spin count exceeded - possible deadlock"

Due to a rare issue with packets that might be out of order in a TCP connection, you might see ESXi hosts intermittently to fail with a purple diagnostic screen and the error `Spin count exceeded - possible deadlock.` In the `vmkernel.log` file, you see a backtrace for errors in the tcpip stack such as:

```
2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bbf0:
[0x42003081b976]Lock_CheckSpinCount@vmkernel#nover+0x26f stack: 0xffffffffffffff8,
0x15a8f9ed9da6c33, 0x3ff, 0x43201ac1efd8, 0x1

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bc40:
[0x420030908c8d]SP_WaitReadLock@vmkernel#nover+0xba stack: 0x43201ac1efd8, 0x43201ac1efdc,
0x0, 0x0, 0x41ffd380b7a0
```

```
2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bc80:
[0x420030908d2a]SPAcqWriteLockWork@vmkernel#nover+0x33 stack: 0x43201ac10f60,
0x420031ce1595, 0x43201cac3b80, 0x420031d4da3b, 0x43201cac3b80

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bca0:
[0x420031ce1594]rw_wlock@(tcpip4)#<None>+0x8d stack: 0x43201cac3b80, 0x41ffd38030b0, 0x6,
0x41ffd380b7a0, 0x43201ac10f60

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bcb0:
[0x420031d4da3a]tcp_usr_attach@(tcpip4)#<None>+0x7b stack: 0x6, 0x41ffd380b7a0,
0x43201ac10f60, 0x43201ac1aff0, 0x453c10e1bd58

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bcf0:
[0x420031cff0a6]socreate@(tcpip4)#<None>+0x1fb stack: 0x58, 0x43201ac1aff0,
0x41ffd380b7a0, 0x1, 0x6

2023-08-28T02:05:27.920Z cpu96:558792334)0x453c10e1bd40:
[0x420031ceb2b6]vmk_socket@(tcpip4)#<None>+0xa3 stack: 0x1, 0x420031ccf047,
0x45dbc1758950, 0x4313d2803210, 0x43201ac01700
```

This issue is resolved in this release.

PR 3252235: ESXi hosts might fail to boot due to a rare deadlock between open and rename operations on objects with parent-child relationship

A rename operation locks the source and destination directories based on the object pointer address with the assumption that the parent object has the lower address. In rare cases, the assumption might not be correct and the rename lock can happen for the child first and then the parent, while the open operation locks the parent first and then the child. As a result, a deadlock between the open and rename operations occurs and ESXi hosts fail to boot.

This issue is resolved in this release.

PR 3313970: ESXi hosts might fail with a purple diagnostic screen due to a write lock of the uplink watchdog

During a regular sanity check, the uplink watchdog might hold a write lock that prevents reads from other services and might cause the ESXi host might fail with a purple diagnostic screen. In the backtrace, you see errors such as:

```
Panic Message: @BlueScreen: NMI IPI: Panic requested by another PCPU. RIPOFF(base):RBP:CS

[0x14e1e0(0x420033000000):0x430201d03440:0xf48] (Src 0x4, CPU14).
```

This issue is resolved in this release. The fix replaces the write lock with a read lock for regular sanity checks.

PR 3331539: Migration between NSX segments with many container logical ports might cause an ESXi host to fail with a purple diagnostic screen

A rare race condition between vSphere vMotion tasks on NSX Segments with many container logical ports might cause an ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3240662: Host Profile compliance check throws incorrect error message "IPv4 vmknic gateway configuration doesn't match the specification"

In the vSphere Client, you might see the error `IPv4 vmknic gateway configuration doesn't match the specification` when running a compliance check on a Host Profile. The error remains even when you remediate the Host Profile. However, the default gateway settings are defined from the Host Customization workflows and you should not see such an error message during compliance checks. Disregard the message, as it does not affect the host profile functions.

This issue is resolved in this release.

PR 3271089: Virtual machines with a lightweight delta (LWD) snapshot might fail to start after a failure of the vmx service

In rare cases, if the vmx service fails during the creation of a LWD snapshot, some partially initialized LWD snapshot files might remain on the datastore. As a result, virtual machines with such LWD snapshots might fail to start due to validation failures.

This issue is resolved in this release.

PR 3304469: vSphere vMotion operations might fail due to a rare issue with no namespaces present in the namespacemgr.db file

When a virtual machine is configured with namespaces and for some reason the namespaces table in the `namespacemgr.db` file is empty in the ESXi host database, migration of such a VM by using vSphere vMotion might fail. In the `vmware.log` file, you see errors such as:

```
vmx - NamespaceMgrCheckpoint: No valid queue found while restoring the namespace events.
The migrate type is 1.
```

This issue is resolved in this release.

PR 3291105: While detaching an Enhanced Networking Stack (ENS) port from an ESXi host, the host might fail with a purple diagnostic screen

During deactivation of ENS in scenarios such as an upgrade or a VNIC configuration change, while detaching an ENS port from an ESXi host with active ENS, the port might be removed from the port list and not be available for further reference, which might cause an invalid memory access error. As a result, the ESXi host fails with a purple diagnostic screen.

This issue is resolved in this release.

PR 3346938: After a NSX Distributed Security installation, vSphere vMotion might not restore a switch security filter on the destination side

When you opt to install the Security Only option of NSX Distributed Security, vSphere vMotion might not restore a switch security filter on the destination side and the Address Resolution Protocol (ARP) fails.

This issue is resolved in this release.

PR 3312150: Failover of VMs on vSphere Virtual Volume datastores might fail due to wrong order of metadata from vSphere API for Storage Awareness (VASA) provider

Certain VASA providers might return metadata info in a different order than what an ESXi host requests. As a result, when VMs on a vSphere Virtual Volume datastore fail over to a recovery site, the VMs cannot reboot on the target site.

This issue is resolved in this release. With the fix, even if a VASA provider returns metadata info in a different order from the ESXi host request, failover succeeds.

PR 3328641: An ESXi host might fail with a purple diagnostic screen due to a rare issue during a read-modify-write (RMW) operation

On 512e software emulated devices, when I/O requests are not multiple of 4096, ESXi runs RMW operations. In such cases, the final write I/O issue path can access the write command frame after the write is issued to the target. If the target completes the write request before the issue path accesses the write frame, the write frame is freed. As a result, you might see a Use-After-Free scenario that might lead to failure of the ESXi host with a purple diagnostic screen.

This issue is resolved in this release.

PR 3332098: Asynchronous write operations to a SMB file share on the vSAN File Service might cause data transfer issues

In rare cases, a race condition during asynchronous write operations to a SMB file share on the vSAN File Service might cause data transfer issues such as truncation.

This issue is resolved in this release.

PR 3256992: vSphere vMotion tasks fail for VMs on port groups with promiscuous mode enabled

A rare issue with corrupted network packets that becomes evident in secure network protocols, where packet data integrity is checked upon receipt, might lead to connectivity issues on port groups with promiscuous mode enabled. As a result, you might see vSphere vMotion tasks failing for VMs on such port groups. You see data integrity errors such as `Failed to decrypt ciphertext` in the backtrace.

This issue is resolved in this release.

PR 3244429: Exit Code 127 error in the hostd service might cause an ESXi host to disconnect temporarily from vCenter

Due to an issue in the open source glibc components, attempts by hostd to process the list of installed I/O filters on an ESXi host might intermittently cause an Exit Code 127 error. In the `/var/run/log/syslog.log` , you see lines such as:

```
2022-10-13T08:00:20.180Z watchdog-hostd[<PID>]: 'hostd ++min=0,swapscope=system' exited after X seconds 127
```

As a result, the ESXi host temporarily disconnects from vCenter until the hostd watchdog restarts the service and connectivity restores. The issue has been observed while loading the `vmwarelwd` I/O filter.

This issue is resolved in this release. ESXi 7.0 Update 3q adds a hostd configuration option that allows you to deactivate an I/O filter without removing it from the vCenter system and skip reporting such filters in the host configuration overhead. To use the option, log in to SSH and complete the following steps:

1. Set the `plugins/hostsvc/report_disabled_filters_in_host_config` option in the hostd configuration to `False` as described in VMware knowledge base article 82227.
2. Deactivate the `vmwarelwd` filter by running the following python script directly on the host:

   ```
   import vmware.vsi as vsi
   vsi.set('/iofilters/statusDisabledEvent', {'filterName': 'vmwarelwd', 'failureReason' : 'workaround'})
   ```

PR 3332691: vSAN IOPS performance data not available for VM multi-writer virtual disk

The following performance charts for a vSAN VM multi-writer virtual disk, under **Monitor** > **vSAN** > **Performance** > **Virtual Disks**, are not available: IOPS, IOPS limit, and Delayed Normalized IOPS. These charts are available only for disks without active multi-writer mode.

This issue is resolved in this release.

PR 3288607: An ESXi host might fail with a purple diagnostic screen due to a rare storage heap corruption in NVMe devices

In rare cases, an I/O thread from a NVMe device, such as deleting a virtual machine from a datastore using NVMe devices, might complete before the High-Performance Plug-in (HPP) claims the device to complete the thread. As a result, HPP tries to access a non-existing thread which leads to a failure of the ESXi host with a purple diagnostic screen and an error such as `PSOD @BlueScreen: PANIC bora/vmkernel/main/dlmalloc.c:4763` .

This issue is resolved in this release.

PR 3273752: ESXi hosts fail with a purple diagnostic screen and a #PF Exception 14 in world 2097479:HELPER_SCSI_ error

After a change in the namespace list for a controller, for example the PsaNvmeController, the update semaphore works as expected, but the change might not complete because no lock is available. As a result, the ESXi host fails with a purple diagnostic screen and a `#PF Exception 14 in world 2097479:HELPER_SCSI_ error` .

This issue is resolved in this release.

PR 3267977: You might see spikes in the latency performance metrics after creating a virtual machine disk snapshot

After you create a virtual machine disk snapshot, you might see latency spikes in the vSphere performance charts. Such unusual spikes are due to the recreation of some internal system objects and the restart of the latency performance counters in the storage subsystem.

This issue is resolved in this release. The fix prevents false latency alarms after taking virtual machine disk snapshots.

PR 3305227: If you do not increase the TCP/IP heap memory limit before installation of NSX-T Data Center kernel modules, ESXi hosts might crash

When you install NSX-T Data Center kernel modules on ESXi hosts with high loads, the pre-allocated TCP/IP heap during boot required for the operation might not be sufficient and cause the ESXi host to fail with a purple diagnostic screen. The issue occurs when the TCP/IP heap cannot grow quickly enough to provide a continuous allocation of 2 MB of memory in case of memory fragmentation on such ESXi hosts. As a result, ESXi hosts might fail with a purple diagnostic screen and a `vmkernel.log` error such as

```
Heap: 3707: Heap tcpip (44384680/1073746344): Maximum allowed growth (1048576) too small for size (1203496)
```

The purple diagnostic screen failure is less likely to occur if you put the ESXi host in maintenance mode before the NSX-T Data Center kernel modules installation, as MM significantly reduces the memory pressure.

This issue is partially resolved in this release. Starting from ESXi 7.0 Update 3, if you are planning an NSX-T Data Center installation, you can increase the `TcpipHeapSize` limit pre-allocated during boot to 128 MB. For example, if you want to increase the `TcpipHeapSize` allocation to the maximum, you can use the following steps:

1. Increase the heap size to 128 MB by using the command `esxcfg-advcfg -s 128 /Net/TcpipHeapSize`
2. Confirm that the heap size is 128 MB: `esxcfg-advcfg -g /Net/TcpipHeapSize`
3. Reboot the ESXi host.

To avoid this issue, you can reboot the ESXi host and install NSX-T Data Center with no VMs running.

PR 3328301: ESXi hosts might fail with a purple diagnostic screen due to a race condition in the High Performance Plug-in (HPP)

Due to a rare race condition in HPP, when a storage path failover and device deletion occur at the same time, ESXi hosts might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3257098: A virtual machine fails with McastFilter_Deactivate error

In very rare cases, when a VM is low on memory, a code path might not initialize all its members on restart and cause the VM to fail with a purple diagnostic screen and an error such as `McastFilter_Deactivate`.

This issue is resolved in this release. Avoid low memory state of VMs to prevent similar issues.

PR 3317448: IPv6 routing disappears after you deactivate router advertisement on an ESXi host and the host loses connectivity

Deactivating IPv6 router advertisements (RA) on the physical network or deselecting the option "Obtain IP Address through Router Advertisement" at the VMkernel level might cause the default route for the VMkernel adapter to disappear, even when you have a static IPv6 address on the adapter. The issue occurs only when the IPv6 prefix of both the static IP address and the prefix specified in the RA message are the same. As a result, ESXi incorrectly removes the route entry for that particular subnet, despite that the static IP address is still active for the same prefix, and the ESXi host loses connectivity.

This issue is resolved in this release. Avoid using the same IPv6 prefix for both a static IP address and addresses that are automatically configured in RA messages to prevent the issue.

PR 3312843: ESXi hosts intermittently disconnect from the vCenter system and the hostd service restarts

If an ESXi host uses only one of the multipath plug-ins, either HPP or NMP, when the hostd service collects telemetry data on scheduled intervals, the call might return a null pointer value. Dereferencing the `nullptr` might lead to a hostd failure, but the service automatically restarts. As a result, you see the ESXi host intermittently disconnected from the vCenter system.

This issue is resolved in this release. The fix adds a `nullptr` check.

PR 3328337: The hostd service might become unresponsive after a restart due to a rare issue with Inter Process Communication (IPC)

If an IPC process has incorrect payload in the IPC packet, for example: an incorrect version in the header, a deadlock in the iSCSI daemon might cause the hostd service to become unresponsive after a hostd restart. As a result, you cannot perform any operations on the affected ESXi host and VMs by using the vSphere Client.

This issue is resolved in this release.

PR 3285491: You cannot use host profiles to configure a path selection policy for disks using Raw Device Mapping

In some cases, when you try to change or configure the path selection policy of multiple virtual machines by using a host profile, the operation fails for VMs using Raw Device Mapping.

This issue is resolved in this release.

PR 3296093:ESXi hosts intermittently fail with a purple diagnostic screen and a PF Exception 14 error

While running an ESXi upgrade, a rare race condition in the device registration during disk initialization might lead to an ESXi host failing with a purple diagnostic screen. In the screen, you see an error such as `@BlueScreen: #PF Exception 14 in world XXXXX:HELPER_SCSI_ IP` and in the backtrace, you see `vmk_ScsiGetDeviceState` and `nmp_DeviceUpdatePathStates`.

This issue is resolved in this release.

PR 3321157: You might see network outages in vSphere systems using Intel i40en physical NICs and with Enhanced data path enabled

On Intel i40en NICs, TSO packets that exceed the Maximum Segment Size (MSS) of 8 segments might cause the NIC to become unresponsive. In rare cases, a TSO packet from a VM or from a vmknic might exceed the 8-segement limit and you might see network outages due to blocked pNIC tx traffic. The issue is more likely to occur in vSphere systems using Intel i40en physical NICs and with Enhanced data path enabled.

This issue is resolved in this release.

PR 3307580: Large TCP segmentation offload (TSO) packets might cause network traffic latency and intermittent loss of connectivity for some virtual machines

Environments with the enhanced data path networking stack mode enabled might see network traffic latency and intermittent loss of connectivity for some virtual machines due to an issue with the handling of large TSO packets.

This issue is resolved in this release.

PR 3275137: Rare data corruption issue in vSphere systems that use service insertion might lead to ESXi host failure

In vSphere systems that use service insertion, an error with the check of the available buffer size before pulling data might lead to data corruption that might cause the ESXi host to fail with a purple diagnostic screen.

This issue is resolved in this release. The fix makes sure that data pull during service insertion runs only if a sufficient buffer exists.

PR 3270210: The Busybox shell on an ESXi host might fail after you disable echo mode

If you enter a command after `stty -echo`, which disables the echo mode on a Busybox sh shell on an ESXi host, the shell might fail with a coredump.

This issue is resolved in this release.

PR 3319535: Virtual machines with independent_nonpersistent disks might become inaccessible after a VM reset

During a reset, a virtual machine with independent_nonpersistent disks deletes existing redo log files and creates a new redo log. The vmx process updates the new .redo settings in-memory, not in the .vmx file, and when the hostd service reads the disk properties from the .vmx file during sync up, it might consider the redo logs inconsistent. As a result, hostd marks the VM as invalid and the VM becomes inaccessible.

This issue is resolved in this release.

PR 3317445: Enhanced Network Datapath (EDP) might reserve too much memory on a large vSphere system and cause resource issues

EDP reservation is linear to the total memory by reserving up to 1.6% of the total. For a VM with high memory reservation in a large vSphere system, such a memory buffer might be too big. For example, if the system has a 100TB of memory, the EDP reservation might be 1.6TB. As a result, you might see resource issues such as not being able to hot-add VNICs to VMs with high memory reservation.

This issue is resolved in this release. The fix sets the EDP reservation limit at 1% of the total memory and puts a 5GB cap on a single memory reservation. You can adjust the memory reservation limit by using the VMKernel boot option `ensMbufPoolMaxMinMB` or by using the following command: `esxcli system settings kernel set -s ensMbufPoolMaxMBPerGB -v <value-in-MB>`. In any case, you must reboot the ESXi host to enable the change.

PR 3283501: SFCB start, stop, and reporting operations fail due to a stale lockfile: /var/run/sfcbd-init.lock

In rare cases, the `sfcbd-init` script, which creates a lockfile `/var/run/sfcbd-init.lock` to prevent multiple instances of the script from running at the same time, receives a SIGPIPE signal, which terminates the script and leaves the lockfile unhandled. As a result, any further attempts to run the script fail because they cannot acquire the lock.

This issue is resolved in this release. The fix adds SIGPIPE to the list of signals handled by the trap command in the `sfcbd-init` script. This ensures that the lock file is cleared even when the script receives a SIGPIPE signal.

PR 3285243: If an NFS server sends a file handle with 0 length during a new directory creation, ESXi hosts might fail with a purple diagnostic screen

On volumes mounted by using NFSv4.1, if the NFS server sends a file handle with length of 0 in response to a new directory request, the ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3317088: You see slow response times in vSphere environments with NVMe SSDs

When a NVMe SSD fails, it does not respond to any commands from the NVMe driver, such as closing outstanding I/Os. As a result, many I/O and NVMe driver commands might remain pending and cause slow response times in the vSphere environment or even failure of upper layer applications.

This issue is resolved in this release. With the fix, the NVMe driver initiates controller or queue reset in case driver commands are not effective, to allow closing of outstanding I/Os.

PR 3302202: You might see placeholders listed in the Guest OS version drop-down menu for new ESXi virtual machines

When creating a new virtual machine, in the **Guest OS version** drop-down menu you might see placeholders such as Windows 12 and Windows Server 2025. You cannot use such placeholders to create new virtual machines.

This issue is resolved in this release.

PR 3289669: You cannot power on a virtual machine after a failed or canceled export of an Open Virtual Format (OVF) file

A rare deadlock caused by a failed or canceled export of a VM as an OVF file might prevent subsequent start of that VM. The VM appears in a **VM_STATE_EXPORTING** state.

This issue is resolved in this release. If the export of an OVF file fails due to a network outage, you cannot prevent the issue, but you can avoid it if you do not manually cancel OVF exports. If you already face the issue, restart the hostd service on the affected ESXi host by either using the SSH command `/etc/init.d/hostd restart` or selecting **Restart Management Agents** under **Troubleshooting options** in the Direct Console User Interface. The restart of the host service stops any operations on the ESXi host.

PR 3313882: Virtual machines and data objects might become inaccessible after an ESXi firewall refresh

In some scenarios, a refresh of the ESXi firewall on vSAN clusters might refer to an incomplete object in the ESXi Configuration Store (ConfigStore) and cause the Reliable Datagram Transport (RDT) and Cluster Monitoring, Membership and Directory Service (CMMDS) firewall rules to be disabled. As a result, some clusters might be isolated and virtual machines and data objects might become inaccessible.

This issue is resolved in this release.

PR 3280714: In the web console of Linux virtual machines, the Caps Lock option does not work consistently

When you enable the Caps Lock option in the web console of a Linux virtual machine, the typing output might not consistently be capital letters.

This issue is resolved in this release.

PR 3287440: ESXi hosts stop responding to tasks from the vSphere Client

Due to a rare race condition with accessing vSphere Distributed Switch data from competing services, ESXi hosts might stop responding to tasks from the vSphere Client. For example, in NSX Data Center for vSphere environments, you might see an error such as `TN Profile attachment to the cluster is in progress` that prevents you from running other tasks.

This issue is resolved in this release.

PR 3282224: VXLAN traffic generated from a guest VM to port 4789 fails

ESXi hosts have VXLAN port 8472 enabled by default and not the UDP port 4789, which is the default for NSX 6.2.3 and later. As a result, traffic to VXLAN port 4789 fails.

This issue is resolved in this release. The fix adds port 4789 to the list of VXLAN ports by default.

PR 3260070: ESXi hosts might fail with a purple diagnostic screen due to a NULL pointer reference in a tardisk object

A NULL pointer violation with `VisorFSTarDoIOInt()` in the backtrace might cause ESXi hosts to fail with a purple diagnostic screen. The issue occurs in the following conditions:

1. A vSphere admin manually logs into the host by using SSH
2. Modifies a tardisk file, for example in `/etc` , without re-writing the file completely
3. Performs an upgrade that replaces a VIB containing that specific file
4. The admin or an ESXi service access the modified file

This issue is resolved in this release.

PR 3284133: ESXi hosts in environments with NVMe PCIe devices might temporarily lose connectivity during collection of diagnostic information

When you use the `vm-support` command to collect information about ESXi systems such as network, storage, and vSAN, logs for the telemetry and persistent events of NVMe PCIe controllers are temporally stored in the ramdisk `/tmp` directory. If your system has many NVMe PCIe devices or the log file is large, the ramdisk `/tmp` directory quickly becomes full. As a result, ESXi hosts in environments with NVMe PCIe devices might temporarily lose connectivity until the `vm-support` collection completes.

This issue is resolved in this release. The fix selects the VMFS datastore with the most free space to store `nvme` logs and compresses each log file to save storage space.

PR 3275377: VBS-enabled Windows VMs might intermittently fail with a blue diagnostic screen on ESXi hosts running on AMD processors

Windows virtual machines with virtualization-based security (VBS) enabled might intermittently fail with a blue diagnostic screen on ESXi hosts running on AMD processors. The BSOD has the following signature:

```
SECURE_KERNEL_ERROR (18b)The secure kernel has encountered a fatal error.
Arguments:
Arg1: 000000000000018c
Arg2: 000000000000100b
Arg3: 0000000000000000
Arg4: 000000000000409b
```

This issue is resolved in this release.

PR 3259205: A stateless ESXi host might lose connection to vCenter after a reboot

During the boot of a stateless ESXi host, in very rare situations, the management vmknic might change unexpectedly and change the IP address of the host. As a result, the host disconnects from vCenter. If you apply a host profile, in the vSphere Client you might see an error such as **Host profile apply failed with error: Error: A specified parameter was not correct: SelectVnic.vnic.Specification.NetStackInstanceKey.**

This issue is resolved in this release.

ESXi-7.0U3sq-23794019-standard

Profile Name	ESXi-7.0U3sq-23794019-standard
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom
Release Date	May 21, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_crx_7.0.3-0.120.23794019 • VMware_bootbank_cpu-microcode_7.0.3-0.120.23794019 • VMware_bootbank_gc_7.0.3-0.120.23794019 • VMware_bootbank_esx-xserver_7.0.3-0.120.23794019 • VMware_bootbank_bmcal_7.0.3-0.120.23794019 • VMware_bootbank_vdfs_7.0.3-0.120.23794019 • VMware_bootbank_native-misc-drivers_7.0.3-0.120.23794019 • VMware_bootbank_trx_7.0.3-0.120.23794019 • VMware_bootbank_vsanhealth_7.0.3-0.120.23794019 • VMware_bootbank_esx-base_7.0.3-0.120.23794019 • VMware_bootbank_vsan_7.0.3-0.120.23794019 • VMware_bootbank_esxio-combiner_7.0.3-0.120.23794019 • VMware_bootbank_esx-ui_2.13.2-22721163 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.120.23794019 • VMware_bootbank_loadesx_7.0.3-0.120.23794019 • VMware_bootbank_esx-update_7.0.3-0.120.23794019 • VMware_locker_tools-light_12.3.5.22544099-23794019

PRs Fixed	3352357, 3340944, 3330942, 3293531, 3368526, 3373896, 3378149, 3331610, 3293308, 3269602, 3293518, 3312311, 3293459, 3293188, 3260854, 3293307, 3302202, 3293541, 3269861, 3296323, 3280714, 3304808, 3293185, 3388772
Related CVE numbers	CVE-2024-22273

This patch updates the following issues:

VMware Tools Bundling Changes in ESXi 7.0 Update 3q

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3q:

- **windows.iso**: VMware Tools 12.3.5 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
- **linux.iso**: VMware Tools 10.3.26 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- VMware Tools 12.3.5 Release Notes
- Earlier versions of VMware Tools
- What Every vSphere Admin Must Know About VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- Updating VMware Tools

ESXi 7.0 Update 3q provides the following security updates:

- The Python library is updated to version 3.8.18.
- The zlib library is updated to version 1.3.
- The cURL library is updated to version 8.4.0.
- The c-ares C library is updated to version 1.19.1.

ESXi 7.0 Update 3q includes the following Intel microcode:

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x7	4/23/2018	Intel Core i7-620LE Processor

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x4003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x5003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x7002703	3/21/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0xe000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x38	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0xd0003b9	9/1/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x1000268	9/8/2023	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	0xb4	9/7/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	0x34	9/7/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	0x4e	9/7/2023	Intel Xeon W-11000E Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	0x2c000321	8/21/2023	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	0x2b000541	8/21/2023	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0xf4	2/23/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0xfa	2/27/2023	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x5d	9/3/2023	Intel Xeon E-2300 Series
Raptor Lake E/HX/S	0xb0671 (06/b7/1)	0x32	0x11e	8/31/2023	Intel Xeon E-2400 Series

ESXi-7.0U3sq-23794019-no-tools

Profile Name	ESXi-7.0U3sq-23794019-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom
Release Date	May 21, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_crx_7.0.3-0.120.23794019 • VMware_bootbank_cpu-microcode_7.0.3-0.120.23794019 • VMware_bootbank_gc_7.0.3-0.120.23794019 • VMware_bootbank_esx-xserver_7.0.3-0.120.23794019 • VMware_bootbank_bmcal_7.0.3-0.120.23794019 • VMware_bootbank_vdfs_7.0.3-0.120.23794019 • VMware_bootbank_native-misc-drivers_7.0.3-0.120.23794019 • VMware_bootbank_trx_7.0.3-0.120.23794019 • VMware_bootbank_vsanhealth_7.0.3-0.120.23794019 • VMware_bootbank_esx-base_7.0.3-0.120.23794019 • VMware_bootbank_vsan_7.0.3-0.120.23794019

	• VMware_bootbank_esxio-combiner_7.0.3-0.120.23794019 • VMware_bootbank_esx-ui_2.13.2-22721163 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.120.23794019 • VMware_bootbank_loadesx_7.0.3-0.120.23794019 • VMware_bootbank_esx-update_7.0.3-0.120.23794019 • VMware_locker_tools-light_12.3.5.22544099-23794019
PRs Fixed	3352357, 3340944, 3330942, 3293531, 3368526, 3373896, 3378149, 3331610, 3293308, 3269602, 3293518, 3312311, 3293459, 3293188, 3260854, 3293307, 3302202, 3293541, 3269861, 3296323, 3280714, 3304808, 3293185, 3388772
Related CVE numbers	CVE-2024-22273

This patch updates the following issues:

ESXi 7.0 Update 3q provides the following security updates:

- The Python library is updated to version 3.8.18.
- The zlib library is updated to version 1.3.
- The cURL library is updated to version 8.4.0.
- The c-ares C library is updated to version 1.19.1.

ESXi 7.0 Update 3q includes the following Intel microcode:

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Broadwell H	0x40671 (06/47/1)	0x22	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x4003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x5003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x7002703	3/21/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0xe000014	9/18/2021	Intel Xeon D-1600 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Skylake H/S	0x506e3 (06/5e/3)	0x36	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x38	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0xd0003b9	9/1/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x1000268	9/8/2023	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	0xb4	9/7/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	0x34	9/7/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	0x4e	9/7/2023	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	0x2c000321	8/21/2023	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	0x2b000541	8/21/2023	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0xf4	2/23/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0xfa	2/27/2023	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x5d	9/3/2023	Intel Xeon E-2300 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Raptor Lake E/HX/S	0xb0671 (06/b7/1)	0x32	0x11e	8/31/2023	Intel Xeon E-2400 Series

ESXi7.0U3q - 23794027

Name	ESXi
Version	ESXi7.0U3q - 23794027
Release Date	May 21, 2024
Category	Bugfix
Affected Components	• ESXi Component - core • ESXi VIBs ESXi Install/Upgrade Component • Network driver for Intel(R) X710/XL710/XXV710/X722 Adapters • VMware Native AHCI Driver
PRs Fixed	3269229, 3336578, 3332098, 3324772, 3337108, 3319535, 3336916, 3331375, 3326805, 3335978, 3267977, 3323978, 3331256, 3332691, 3313970, 3312843, 3309601, 3317598, 3323119, 3326739, 3317618, 3244429, 3328641, 3328638, 3328337, 3326300, 3329238, 3328301, 3297696, 3296093, 3317448, 3285491, 3276174, 3297629, 3314959, 3309482, 3320147, 3297625, 3297729, 3311303, 3297704, 3309472, 3297749, 3298709, 3320949, 3310432, 3297774, 3302255, 3270210, 3311302, 3257098, 3311831, 3309603, 3317088, 3321157, 2964964, 3305227, 3318350, 3256083, 3269969, 3317445, 3314400, 3267704, 2760003, 3313882, 3243360, 3293469, 3284876, 3265330, 3303842, 3303855, 3293093, 3309148, 3307580, 3301661, 3304469, 3260297, 3260070, 3297409, 3252235, 3287748, 3306033, 3273752, 3288607, 3289238, 3284916, 3303694, 3284133, 3273653, 3298508, 3289605, 3289669, 3291198, 3240347, 3280468, 3285518, 3283501, 3275377, 3267449, 3282267, 3256992, 3251790, 3275137, 3240662, 3259035, 3259205, 3266912, 3282224, 3273653, 3346924, 3346935, 3346816, 3237506, 3331539, 3271089, 3291105, 3346938, 3312150, 3284149, 3266231, 3317204, 3297607, 3281791
Related CVE numbers	CVE-2024-22273

This patch resolves the issues listed in ESXi-7.0U3q-23794027-standard.

ESXi7.0U3sq - 23794019

Name	ESXi
Version	ESXi7.0U3sq - 23794019
Release Date	May 21, 2024
Category	Security
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • ESXi Tools Component

PRs Fixed	3352357, 3340944, 3330942, 3293531, 3368526, 3373896, 3378149, 3331610, 3293308, 3269602, 3293518, 3312311, 3293459, 3293188, 3260854, 3293307, 3302202, 3293541, 3269861, 3296323, 3280714, 3304808, 3293185
Related CVE numbers	CVE-2024-22273

This patch resolves the issues listed in ESXi-7.0U3sq-23794019-standard.

Known Issues

Virtual Machine Management Issues

Compatibility check for assignable hardware might fail even when no external device is in use

In some cases, when you revert a virtual machine with an assignable hardware (AH) device, such as a GPU resource, to a snapshot when the VM did not have the AH device, some stale bindings might remain. As a result, you see compatibility checks on the reverted VM failing with an error such as `InsufficientResourcesFault for pciPassthru0` , even though the GPU resource is no longer attached.

Workaround: To avoid the issue, for ESXi version 7.x, revert virtual machines with AH or passthrough devices only from snapshots you take from powered off VMs. If you already face the issue, restart the hostd service to release stale bindings and start GPU VMs. Alternatively, upgrade your hosts to ESXi version 8.0 or later.

Known Issues from Previous Releases

For a list of known issues from previous releases, see VMware ESXi 7.0 Update 3p Release Notes.

VMware ESXi 7.0 Update 3p Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues from Previous Releases

Introduction

VMware ESXi 7.0 Update 3p | 11 APR 2024 | Build 23307199 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3p, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3p. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

This release resolves CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0006.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3p Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3o Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3n Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3m Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3l Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Patches Contained in This Release

This release of ESXi 7.0 Update 3p delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3p-23307199-depot.zip
Build:	23307199
Download Size:	381.3 MB
md5sum:	9b04d3fb0cbda95ba2dd06a042971d56
sha256checksum:	f407cf873d191c453ff805b04f75398874bce63120443ce835a2da28977977b1
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.110.23307199	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.110.23307199	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3p-23307199	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3p-23307199-standard
ESXi-7.0U3p-23307199-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi7.0U3p - 23307199	MAR 05 2024	Security	Security only image

For information about the individual components and bulletins, see the Resolved Issues section.

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.110.23307199

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_vsan_7.0.3-0.110.23307199 • VMware_bootbank_esxio-combiner_7.0.3-0.110.23307199 • VMware_bootbank_crx_7.0.3-0.110.23307199 • VMware_bootbank_vsanhealth_7.0.3-0.110.23307199 • VMware_bootbank_trx_7.0.3-0.110.23307199 • VMware_bootbank_vdfs_7.0.3-0.110.23307199 • VMware_bootbank_native-misc-drivers_7.0.3-0.110.23307199 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.110.23307199 • VMware_bootbank_bmcal_7.0.3-0.110.23307199 • VMware_bootbank_esx-xserver_7.0.3-0.110.23307199 • VMware_bootbank_esx-base_7.0.3-0.110.23307199 • VMware_bootbank_cpu-microcode_7.0.3-0.110.23307199 • VMware_bootbank_gc_7.0.3-0.110.23307199
PRs Fixed	N/A
CVE numbers	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

This patch updates the `esx-base` VIB. Due to their dependency with the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `trx`, `vdfs`, `native-misc-drivers`, `esx-dvfilter-generic-fastpath`, `bmcal`, `esx-xserver`, `esx-base`, `cpu-microcode` , and `gc` . This patch resolves the following issue:

This release resolves CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0006.

esx-update_7.0.3-0.110.23307199

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.110.23307199 • VMware_bootbank_esx-update_7.0.3-0.110.23307199
PRs Fixed	N/A
CVE numbers	N/A

Due to their dependency on the `esx-base` VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: `loadesx` and `esx-update` .

ESXi-7.0U3p-23307199-standard

Profile Name	ESXi-7.0U3p-23307199-standard
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom, Inc.
Release Date	March 05, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vsan_7.0.3-0.110.23307199 • VMware_bootbank_esxio-combiner_7.0.3-0.110.23307199 • VMware_bootbank_crx_7.0.3-0.110.23307199 • VMware_bootbank_vsanhealth_7.0.3-0.110.23307199 • VMware_bootbank_trx_7.0.3-0.110.23307199 • VMware_bootbank_vdfs_7.0.3-0.110.23307199 • VMware_bootbank_native-misc-drivers_7.0.3-0.110.23307199 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.110.23307199 • VMware_bootbank_bmcal_7.0.3-0.110.23307199 • VMware_bootbank_esx-xserver_7.0.3-0.110.23307199 • VMware_bootbank_esx-base_7.0.3-0.110.23307199 • VMware_bootbank_cpu-microcode_7.0.3-0.110.23307199 • VMware_bootbank_gc_7.0.3-0.110.23307199 • VMware_bootbank_loadesx_7.0.3-0.110.23307199 • VMware_bootbank_esx-update_7.0.3-0.110.23307199
PRs Fixed	N/A
Related CVE numbers	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255

This patch updates the following issue:

This release resolves CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0006.

ESXi-7.0U3p-23307199-no-tools

Profile Name	ESXi-7.0U3p-23307199-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	VMware by Broadcom, Inc.
Release Date	March 05, 2024
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vsan_7.0.3-0.110.23307199 • VMware_bootbank_esxio-combiner_7.0.3-0.110.23307199 • VMware_bootbank_crx_7.0.3-0.110.23307199 • VMware_bootbank_vsanhealth_7.0.3-0.110.23307199 • VMware_bootbank_trx_7.0.3-0.110.23307199 • VMware_bootbank_vdfs_7.0.3-0.110.23307199 • VMware_bootbank_native-misc-drivers_7.0.3-0.110.23307199 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.110.23307199 • VMware_bootbank_bmcal_7.0.3-0.110.23307199 • VMware_bootbank_esx-xserver_7.0.3-0.110.23307199 • VMware_bootbank_esx-base_7.0.3-0.110.23307199 • VMware_bootbank_cpu-microcode_7.0.3-0.110.23307199 • VMware_bootbank_gc_7.0.3-0.110.23307199 • VMware_bootbank_loadesx_7.0.3-0.110.23307199 • VMware_bootbank_esx-update_7.0.3-0.110.23307199
PRs Fixed	N/A
Related CVE numbers	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255

This patch updates the following issue:

This release resolves CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0006.

ESXi7.0U3p - 23307199

Name	ESXi
Version	ESXi7.0U3p - 23307199
Release Date	March 05, 2024
Category	Security
Affected Components	• ESXi Component - core ESXi

	• ESXi Install/Upgrade
PRs Fixed	N/A
Related CVE numbers	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255

This patch resolves the issues listed in ESXi-7.0U3p-23307199-standard.

Known Issues from Previous Releases

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Corrupted VFAT partitions from a vSphere 6.7 environment might cause upgrades to ESXi 7.x to fail

Due to corrupted VFAT partitions from a vSphere 6.7 environment, repartitioning the boot disks of an ESXi host might fail during an upgrade to ESXi 7.x. As a result, you might see the following errors:

When upgrading to ESXi 7.0 Update 3l, the operation fails with a purple diagnostic screen and/or an error such as:

- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to calculate size for temporary Ramdisk: <error>.`
- `An error occurred while backing up VFAT partition files before re-partitioning: Failed to copy files to Ramdisk: <error>.`
  If you use an ISO installer, you see the errors, but no purple diagnostic screen.

When upgrading to an ESXi 7.x version earlier than 7.0 Update 3l, you might see:

- Logs such as `ramdisk (root) is full` in the `vmkwarning.log` file.
- Unexpected rollback to ESXi 6.5 or 6.7 on reboot.
- The `/bootbank`,`/altbootbank`, and ESX-OSData partitions are not present.

Workaround: You must first remediate the corrupted partitions before completing the upgrade to ESXi 7.x. For more details, see VMware knowledge base article 91136.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the
requirement cannot be satisfied within the ImageProfile. Please refer to the log file for
more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
```

```
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
 The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
 Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s).`

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU.`

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer.`

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network` . This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration

will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Set-VMHostService -policy "off"$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx` , the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1` .

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set
--tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer":
{ "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"` , run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability

- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.

7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists`. The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command:
   `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command:
   `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command:
   `esxcli network firewall load.`
5. Start the hostd service by using the command:
   `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats`, you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835`.

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0`.

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set` **-o** `/USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.
2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

vSAN Issues

PR 2962316: vSAN File Service does not support NFSv4 delegations

vSAN File Service does not support NFSv4 delegations in this release.

Workaround: None

PR 3235496: Applications on a vSAN cluster become intermittently unresponsive

If the advanced option `preferHT` is enabled on an AMD server in a vSAN cluster, the virtual CPUs of a virtual machine run on the same last level cache. When the virtual CPUs are all very busy and an NVMe thread to handle I/Os happens to run also on the same last level cache, the NVMe thread takes very long to complete, because it competes for CPU resources with the busy VMs. As a result, the I/O latency is very high and might lead to intermittent unresponsiveness of storage and applications on the vSAN cluster. In the backlog, you see errors such as `Lost access to volume <uuid> due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.`

Workaround: Use the command `esxcli system settings advanced set -o /Misc/vmknvmeCwYield -I 0` to avoid competition between the NVMe completion queue and busy virtual CPUs.

VMware ESXi 7.0 Update 3o Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Product Support Notices
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues

Introduction

VMware ESXi 7.0 Update 3o | 28 SEP 2023 | Build 22348816
Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3o, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3o. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- ESXi 7.0 Update 3o adds support for vSphere Quick Boot to multiple servers, including:
  - Dell
    - PowerEdge XR4510c
    - PowerEdge XR4520c
    - PowerEdge XR5610
    - PowerEdge XR7620
    - PowerEdge XR8620t
    - R6615 vSAN Ready Node
    - R7615 vSAN Ready Node
    - VxRail VD-4510c
    - VxRail VD-4520c
  - Lenovo
    - ThinkSystem SR635 V3
    - ThinkSystem SR645 V3
    - ThinkSystem ST650 V3
    - ThinkSystem SR655 V3
  - HPE
    - Alletra 4120
    - Cray XD220v
    - ProLiant DL320 Gen11
    - ProLiant DL380a Gen11
    - ProLiant DL560 Gen11
    - ProLiant ML110 Gen11
    - ProLiant DL360 Gen11
    - ProLiant DL380 Gen11
    - ProLiant ML350 Gen11
- ESXi 7.0 Update 3o adds support for vSphere Quick Boot to several drivers, including:
  - Intel
    - QuickAssist Technology (QAT)
    - Dynamic Load Balancer (DLB)
  - Cisco
    - NENIC_ENS

  For the full list of supported servers and drivers, see the VMware Compatibility Guide.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3n Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3m Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3l Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Product Support Notices

Support for spaces in organizational units (OUs) names: With ESXi 7.0 Update 3o, vSAN File Service supports spaces in organizational units (OUs) names.

Patches Contained in This Release

This release of ESXi 7.0 Update 3o delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3o-22348816-depot.zip
Build:	22348816
Download Size:	574.5 MB
md5sum:	2dc3fe97405d94a12c3a7b14570e24c1
sha256checksum:	42594bd42b9cf2f7d002780d8fee9062a61567a9f3f1a0675726a6f29075d607
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.105.22348816	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.105.22348816	Bugfix	Critical
VMware Native AHCI Driver	VMware-ahci_2.0.11-2vmw.703.0.105.22348816	Bugfix	Critical
SMARTPQI LSU Management Plugin	Microchip-smartpqiv2-plugin_1.0.0-9vmw.703.0.105.22348816	Bugfix	Critical
Non-Volatile memory controller driver	VMware-NVMe-PCIe_1.2.3.16-3vmw.703.0.105.22348816	Bugfix	Critical
Avago (LSI) Native 12Gbps SAS MPT Driver	Broadcom-lsi-msgpt3_17.00.12.00-2vmw.703.0.105.22348816	Bugfix	Critical
Intel NVME Driver with VMD Technology	Intel-Volume-Mgmt-Device_2.7.0.1157-3vmw.703.0.105.22348816	Bugfix	Critical
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.100.22348808	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.100.22348808	Security	Critical
ESXi Tools Component	VMware-VM-Tools_12.2.6.22229486-22348808	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3o-22348816	Bugfix	Critical	Security and Bugfix
ESXi70U3so-22348808	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3o-22348816-standard
ESXi-7.0U3o-22348816-no-tools
ESXi-7.0U3so-22348808-standard
ESXi-7.0U3so-22348808-no-tools

ESXi Image

Name and Version	Release Date	Category	Details
ESXi7.0U3o - 22348816	SEP 28 2023	Bugfix	Security and Bugfix image
ESXi7.0U3so - 22348808	SEP 28 2023	Security	Security only image

For information about the individual components and bulletins, see the Resolved Issues section.

Patch Download and Installation

Download this patch from the Broadcom Support Portal.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see How to Download a ZIP file for ESXi Patches and Updates, Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

The resolved issues are grouped as follows:

ESXi_7.0.3-0.105.22348816

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_gc_7.0.3-0.105.22348816 • VMware_bootbank_native-misc-drivers_7.0.3-0.105.22348816 • VMware_bootbank_vsanhealth_7.0.3-0.105.22348816 • VMware_bootbank_crx_7.0.3-0.105.22348816 • VMware_bootbank_esx-xserver_7.0.3-0.105.22348816 • VMware_bootbank_vdfs_7.0.3-0.105.22348816

	• VMware_bootbank_cpu-microcode_7.0.3-0.105.22348816 • VMware_bootbank_esx-base_7.0.3-0.105.22348816 • VMware_bootbank_vsan_7.0.3-0.105.22348816 • VMware_bootbank_esxio-combiner_7.0.3-0.105.22348816 • VMware_bootbank_esx-ui_2.11.2-21988676 • VMware_bootbank_bmcal_7.0.3-0.105.22348816 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.105.22348816 • VMware_bootbank_trx_7.0.3-0.105.22348816
PRs Fixed	3244098, 3216958, 3245763, 3242021, 3246132, 3253205, 3256804, 3239170, 3251981, 3215370, 3117615, 3248478, 3252676, 3235496, 3238026, 3236064, 3224739, 3224306, 3223755, 3216958, 3233958, 3185125, 3219264, 3221620, 3218835, 3185560, 3221099, 3211625, 3221860, 3228586, 3224604, 3223539, 3222601, 3217258, 3213041, 3216522, 3221591, 3216389, 3220004, 3217633, 3216548, 3216449, 3156666, 3181574, 3180746, 3155476, 3211807, 3154090, 3184008, 3183519, 3183519, 3209853, 3100552, 3187846, 3113263, 3176350, 3185827, 3095511, 3184425, 3186351, 3186367, 3154090, 3158524, 3181601, 3180391, 3180283, 3184608, 3181774, 3155476, 3163361, 3182978, 3184368, 3160456, 3164575, 3181901, 3184871, 3166818, 3157195, 3164355, 3163271, 3112194, 3161690, 3261925, 3178589, 3178721, 3162963, 3168950, 3159168, 3158491, 3158866, 3096769, 3165374, 3122037, 3098760, 3164439, 3161473, 3162790, 3100030, 3096974, 3161473, 3165651, 3083007, 3118240, 3151076, 3118402, 3160480, 3156627, 3158531, 3162499, 3158512, 3053430, 3153395, 3117615, 3099192, 3158508, 3115870, 3119834, 3158220, 3110401, 2625439, 3099357, 3152811, 3108979, 3120165
CVE numbers	N/A

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `gc`, `native-misc-drivers`, `vsanhealth`, `crx`, `esx-xserver`, `vdfs`, `cpu-microcode`, `esx-base`, `vsan`, `esxio-combiner`, `esx-ui`, `bmcal`, `esx-dvfilter-generic-fastpath` and `trx` VIBs to resolve the following issues:

PR 3253205: Static IPv6 gateway disappears in 18 hours

If you configure a static IPv6 gateway address in your vSphere environment, such gateways might no longer exist in up to 18 hours due to a timeout.

This issue is resolved in this release. The fix removes the existing timeout for static gateways.

PR 3272532: You see speed as Half Duplex after changing the speed from Auto to Full on a VMNIC

In some cases, length checks during the parsing of duplex TLVs in an environment with active Cisco Discovery Protocol (CDP) might fail. As a result, when you change the speed from **Auto** to **Full** on a physical NIC on peer devices you do not see the real duplex value in the TLV under the neighbor information, but the default Half Duplex value.

This issue is resolved in this release.

PR 3251981: An NFSv4.1 file might appear to be empty even though it contains data

When you open an existing NFSv4.1 file with write only access, if for some reason the NFS client opens again the same file with read only access, read operations from the client might return no data although the file is not empty.

This issue is resolved in this release.

PR 3116601: When you override the default gateway for the vSAN VMkernel adapter on an ESXi host, the vSphere HA agent on the host displays as inaccessible

In some cases, when you override the default gateway for the vSAN VMkernel adapter on an ESXi host, the Fault Domain Manager (FDM), which is the agent that vSphere HA deploys on ESX hosts, might stop receiving Internet Control Message Protocol (ICMP) pings. As a result, FDM might issue false cluster alarms that the vSphere HA agent on the host cannot reach some management network addresses of other hosts.

This issue is resolved in this release.

PR 3251801: vSphere vMotion operation from a 6.7.x ESXi host with an Intel Ice Lake CPU fails with msg.checkpoint.cpucheck.fail

vSphere vMotion operations by using either the vSphere Client or VMware Hybrid Cloud Extension (HCX) from an Intel Ice Lake CPU host running ESXi 6.7.x fails with an error such as `msg.checkpoint.cpucheck.fail` . In the vSphere Client, you see a message that cpuid.PSFD is not supported on the target host. In HCX, you see a report such as `A general system error occurred: vMotion failed:` .

This issue is resolved in this release.

PR 3224739: You see alarms for dropped syslog messages

If the network throughput of your vSphere system does not align with the speed at which log messages are generated, some of the log messages sent to the remote syslog server might drop. As a result, in the vSphere Client you see host errors of type `Triggered Alarm` and in the logs, you see warnings such as `ALERT: vmsyslog logger xxxx:514 lost yyyy log messages` .

This issue is resolved in this release. The fix improves the network logging performance of the logging service to reduce the number of such lost log messages.

PR 3247027: If any failure occurs during a vSphere vMotion migration of NVIDIA virtual GPU (vGPU) VM, the destination ESXi host might fail with a purple diagnostic screen

In very rare cases, if any type of failure occurs during a vSphere vMotion migration of a vGPU VM, the vMotion operation is marked as a failure while a specific internal operation is in progress. As a result, the destination ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3095511: The SFCB service intermittently fails and generates "sfcb-vmware_bas-zdump" files on multiple ESXi hosts

In very rare cases, when the SFCB service tries to access an uninitialized variable, the service might fail with dump file such as `sfcb-vmware_bas-zdump.000` . The issue occurs because accessing an uninitialized variable can cause the SFCB process to keep requesting memory until it exceeds the heap allocation.

This issue is resolved in this release.

PR 3256804: File server loses connectivity after failover when running vSAN File Service on NSX overlay network

If vSAN File Service is running on an NSX overlay network, the file server might lose connectivity after it fails over from one agent VM to another agent VM. The file server can failover when reconfiguring file service domain from such without Active Directory(AD) to such with AD, or if vSAN detects unhealthy behavior in the file server, file share, or AD server. If file server connectivity is lost after a failover, File Service clients cannot access the file share. The following health warning might be reported:

```
One or more DNS servers is not reachable.
```

This issue is resolved in this release.

PR 3217633: vSAN management service on the orchestration host malfunctions during vCenter restart

This issue can occur on vSAN clusters where vCenter is deployed. If multiple cluster shutdown operations are performed, the `/etc/vmware/vsan/vsanperf.conf` file on the orchestration host can contain two versions of the following management VM: `vc_vm_moIdvc_vm_moid`. These configuration options conflict with each other and can cause the vSAN management service to malfunction.

This issue is resolved in this release.

PR 3224306: When you change the ESXi syslog setting syslog.global.logDir, if syslog.global.logDirUnique is active, you might see 2 levels of <hostname> subdir under the logdir path

After upgrading an ESXi host to 7.0 Update 3c and later, if you change the syslog setting `syslog.global.logDir` and the `syslog.global.logDirUnique` setting is active, you might see 2 levels of `<hostname>` subdirs under the `logdir` path on the host. The `syslog.global.logDirUnique` setting is useful if the same NFS directory is configured as the `Syslog.global.LogDir` by multiple ESXi hosts, as it creates a subdirectory with the name of the ESXi host under `logdir`.

This issue is resolved in this release.

PR 3223755: ESXi syslog daemon fails to resume transmitting logs to the configured SSL remote syslog server once a drop in the network connectivity restores

If a remote SSL syslog server temporarily loses connectivity, the ESXi syslog daemon might fail to resume transmitting logs after connectivity restores and you must restart the service to re-activate transmissions. The issue occurs due to some unhandled exceptions while the ESXi syslog daemon tries to restore connection to the SSL remote syslog server.

This issue is resolved in this release. The fix adds a generic catch for all unhandled exceptions.

PR 3185536: vSAN cluster remediation error after vCenter upgrade to 7.0 Update 3

When you upgrade vCenter from version 6.5.x to 7.0 Update 3, and reconfigure the vSAN cluster, a vSAN cluster remediation is triggered, but in some cases fails.

This issue is resolved in this release.

PR 3110401: The Explicit Congestion Notification (ECN) setting is not persistent on ESXi host reboot

ECN, specified in RFC 3168, allows a TCP sender to reduce the transmission rate to avoid packet drops and is activated by default. However, if you change the default setting, or manually deactivate ECN, such changes to the ESXi configuration might not persist after a reboot of the host.

This issue is resolved in this release.

PR 3153395: Upon refresh, some dynamic firewalls rules might not persist and lead to vSAN iSCSI Target service failure

If you frequently run the command `esxcli network firewall refresh`, a race condition might cause some dynamic firewalls rules to be removed upon refresh or load. As a result, some services such as the vSAN iSCSI Target daemon, which provides vSAN storage with iSCSI protocol, might fail.

This issue is resolved in this release.

PR 3096769: You see high latency for VM I/O operations in a vSAN cluster with Unmap activated

This issue affects vSAN clusters with Unmap activated. A problem in Unmap handling in LSOM creates log congestion. The log congestion can cause high VM I/O latency.

This issue is resolved in this release.

PR 3163361: The Audit Record Storage Capacity parameter does not persist across ESXi host reboots

After an ESXi host reboot, you see the **Audit Record Storage Capacity** parameter restored to the default value of 4 MiB, regardless of any previous changes.

This issue is resolved in this release.

PR 3162496: If the Internet Control Message Protocol (ICMPA) is not active, ESXi host reboot might take long after upgrading to vSphere 8.0 and later

If ICMPA is not active on the NFS servers in your environment, after upgrading your system to vSphere 8.0 and later, ESXi hosts reboot might take an hour to complete, because restore operations for NFS datastores fail. NFS uses the `vmkping` utility to identify reachable IPs of the NFS servers before executing a mount operation and when ICMP is not active, mount operations fail.

This issue is resolved in this release. To remove dependency on the ICMP protocol to find reachable IPs, the fix adds socket APIs to ensure that IPs on a given NFS server are available.

PR 3220004: VBS-enabled Windows VMs might fail with a blue diagnostic screen when an ESXi host is under memory pressure

Windows VMs with virtualization-based security (VBS) enabled might intermittently fail with a blue diagnostic screen during memory-heavy operations such as deleting snapshots or consolidating disks. The BSOD has the following signature:

```
DRIVER_VERIFIER_DMA_VIOLATION (e6)
An illegal DMA operation was attempted by a driver being verified.
```

Arguments:

```
Arg1: 0000000000000026, IOMMU detected DMA violation.
Arg2: 0000000000000000, Device Object of faulting device.
Arg3: xxxxxxxxxxxxxxxx, Faulting information (usually faulting physical address).
Arg4: 0000000000000008, Fault type (hardware specific).
```

This issue is resolved in this release.

PR 3162905: ESXi hosts might intermittently disconnect from vCenter in case of memory outage

In rare cases, if vCenter fails to allocate or transfer active bitmaps due to an alert for insufficient memory for any reason, the hostd service might repeatedly fail and you cannot reconnect the host to the vCenter.

This issue is resolved in this release. The fix makes sure that in such cases you see an error rather than the hostd service failure.

PR 3108979: Staging ESXi patches and ESXi upgrade tasks might become indefinitely unresponsive due to a log buffer limit

If a large string or log exceed the python log buffer limit of 16K, the logger becomes unresponsive. As a result, when you stage ESXi patches on a host by using the vSphere Client, the process responsible for completing the staging task on ESXi might become indefinitely unresponsive. The task times out and reports an error. The issue occurs also when you remediate ESXi hosts by using a patch baseline.

This issue is resolved in this release. The fix breaks the large input string into smaller chunks for logging.

PR 3219264: vSAN precheck for maintenance mode or disk decommission doesn't list objects that might lose accessibility

This issue affects objects with resyncing components, and some components reside on a device to be removed or placed into maintenance mode. When you run a precheck with the **No-Action** option, the precheck does not evaluate the object correctly to report it in the `inaccessibleObjects` list.

This issue is resolved in this release. Precheck includes all affected objects in the `inaccessibleObjects` list.

PR 3186545: Vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable

Some third-party tools for vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable.

This issue is resolved in this release.

PR 3221591: ESXi NVMe/TCP initiator fails to recover paths after target failure recovery

When a NVMe/TCP target recovers from a failure, ESXi cannot recover the path.

This issue is resolved in this release.

PR 3186351: You see an override flag of NIC teaming, security, or traffic shaping policy on a portgroup unexpectedly enabled post an ESXi host reboot

In some cases, a networking configuration might not persist in the ESXi ConfigStore and you see an override flag of NIC teaming, security, or traffic shaping policy on a portgroup unexpectedly enabled post an ESXi host reboot.

This issue is resolved in this release.

PR 3162790: The sfcb daemon might fail with a core dump while installing a third-party CIM provider

The sfcb daemon might try to access already freed memory when registering a CIM provider and fail with a core dump while installing a third-party CIM provider, such as Dell OpenManage Server Administrator for example.

This issue is resolved in this release.

PR 3157195: ESX hosts might fail with a purple diagnostic screen and an error NMI IPI: Panic requested by another PCPU

The resource pool cache is a VMFS specific volume level cache that stores the resource clusters corresponding to the VMFS volume. While searching for priority clusters, the cache flusher workflow iterates through a large list of cached resource clusters, which can cause lockup of the physical CPUs. As a result, ESX hosts might fail with a purple diagnostic screen. In the `logDump` file, you see an error such as:

```
^[[7m2022-10-22T07:56:47.322Z cpu13:2101160)WARNING: Heartbeat: 827: PCPU 0 didn't have a heartbeat for 7 seconds, timeout is 14, 1 IPIs sent; *may* be locked up.^[[0m^
```

```
[[31;1m2022-10-22T07:56:47.322Z cpu0:2110633)ALERT: NMI: 710: NMI IPI: RIPOFF(base):RBP:CS
```

This issue is resolved in this release.

PR 3230493: If a delta sync runs while the target vSphere Replication server is not active, Windows virtual machines might become unresponsive

If the target Sphere Replication server is not active during a delta sync, the synchronization process cannot complete and Windows virtual machines become unresponsive.

This issue is resolved in this release. The fix makes sure that no delta sync jobs start when a Sphere Replication server is not active.

PR 3122037: ESXi ConfigStore database fills up and writes fail

Stale data related to block devices might not be deleted in time from the ESXi ConfigStore database and cause an out of space condition. As a result, write operations to ConfigStore start to fail. In the backtrace, you see logs such as:

```
2022-12-19T03:51:42.733Z cpu53:26745174)WARNING: VisorFSRam: 203: Cannot extend visorfs file /etc/vmware/configstore/current-store-1-journal because its ramdisk (configstore) is full .
```

This issue is resolved in this release.

PR 3246132: You see a system clock drift on an ESXi host after synchronization with the NTP server fails

If connectivity between the NTP server and an ESXi host is delayed for some reason, the system clock on the ESXi host might experience a drift. When you run the `vsish` command `vsish -e get /system/ntpclock/clockData` , you might see a large negative value for the `adjtime` field. For example:

```
NTP clock data {
...  adjtime() (usec):-309237290312 <<<<<<
...
}
```

This issue is resolved in this release.

PR 3185560: vSphere vMotion operations for virtual machines with swap files on a vSphere Virtual Volumes datastore intermittently fail after a hot extend of the VM disk

vSphere vMotion operations for virtual machines with swap files on a vSphere Virtual Volumes datastore might fail under the following circumstances:

A VM that runs on ESXi host A is migrated to ESXi host B, then the VM disk is hot extended, and the VM is migrated back to ESXi host A. The issue occurs due to stale statistics about the swap virtual volume.

This issue is resolved in this release.

PR 3236207: You cannot unmount an NFS v3 datastore from a vCenter system because the datastore displays as inaccessible

While unmounting an NFSv3 datastore from a vCenter system by using either the vSphere Client or ESXCLI, you might see the datastore either as inaccessible, or get an `Unable to Refresh` error. The issue occurs when a hostd cache refresh happens before NFS deletes the mount details from ConfigStore, which creates a rare race condition.

This issue is resolved in this release.

PR 3236064: Compliance or remediation scans by using vSphere Lifecycle Manager might take long on ESXi hosts with a large number of datastores

Compliance or remediation scans by using vSphere Lifecycle Manager include an upgrade precheck that lists all volumes attached to an ESXi host, their free space, versions, and other details. If a host has many datastores attached, each with a large capacity, the precheck can take long. The time is multiplied by the number of baselines attached to the cluster or host.

This issue is resolved in this release. If you already face the issue, disconnect the attached datastores while performing the remediation or compliance scans and reattach them after the operations complete.

PR 3245763: During a vSphere vMotion operation, destination ESXi hosts with a Distributed Firewall (DFW) enabled might fail with a purple diagnostic screen

If the destination host in a vSphere vMotion operation has a DFW enabled, a rare race condition might cause the host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3158866: Virtual machines might become unresponsive during VMFS volume expansion due to a Logical Volume Manager (LVM) check

If a VMFS volume expansion operation happens during a LVM probe to update volume attributes, such as the size of the VMFS partition backing of the VMFS volume, the current size of the VMFS volume might not match the LVM metadata on the disk. As a result, LVM marks such a volume offline and virtual machines on that volume become unresponsive.

This issue is resolved in this release. The fix improves Input Output Control (IOCTL) to speed up the update of device attributes and avoid such cases.

PR 3152717: vSphere Auto Deploy workflows might fail after an upgrade to vCenter Server 7.0 Update 3j or later

Due to a networking issue in reverse proxy configuration environments, vSphere Auto Deploy workflows might fail after an upgrade to vCenter Server 7.0 Update 3j or later. In the ESXi management console and in the `/var/log/vmware/rbd/rbd-cgi.log file` you see an HTTP client error.

This issue is resolved in this release. The fix makes sure Auto Deploy workflows run successfully in reverse proxy configuration environments.

PR 3185125: Virtual SLIT table not populated for the guest OS when using sched.nodeX.affinity

When you specify virtual NUMA node affinity, the vSLIT table might not be populated and you see the following error in `vmware.log : vSLIT: NumaGetLatencyInfo failed with status: 195887107.`

This happens when setting node affinity as follows:

```
numa.slit.enable = "TRUE"

sched.node0.affinity = 0

sched.node1.affinity = 1

...sched.nodeN.affinity = N
```

This issue is resolved in this release. If you already face the issue, specify VCPU affinity to physical CPUs on the associated NUMA nodes, instead of node affinity.

For example:

```
numa.slit.enable = "TRUE"

sched.vcpu0.affinity = "0-7"

sched.vcpu1.affinity = "0-7"

...sched.vcpuN.affinity = "Y-Z"
```

PR 3181774: You do not see an error when you attach a CBT enabled FCD to a VM with CBT disabled

Attaching a First Class Disk (FCD) with Changed Block Tracking (CBT) to a VM with CBT disabled does not throw a detailed error, but the operation cannot take effect. In the backtrace, you might see an error message such as `InvalidState` , which is generic and does not provide details on the issue.

This issue is resolved in this release. The fix adds the error message `Cannot attach a CBT enabled fcd: {path} to CBT disabled VM.` to the logs of the hostd service and adds a status message for the task in the vSphere Client.

PR 3185827: You see trap files in a SNMP directory under /var/spool even though SNMP is not enabled

After the hostd service starts, for example after an ESXi host reboot, it might create a SNMP directory under `/var/spool` and you see many `.trp` files to pile in this directory.

This issue is resolved in this release. The fix makes sure that the directory `/var/spool/snmp` exists only when SNMP is enabled.

PR 3082867: An ESXi host might fail with a purple diagnostic screen after a replicated virtual machine migrates to the host

In some environments, when a replicated virtual machine migrates to a certain ESXi host, during a full sync, some `SCSI WRITE` commands might target address ranges past the end of the transfer map. As a result, the ESXi host might fail with a purple diagnostic screen and a backtrace such as:

```
#0 DLM_free (msp=0x43238f2c9cc0, mem=mem@entry=0x43238f6db860, allowTrim=allowTrim@entry=1
'\001') at bora/vmkernel/main/dlmalloc.c:4924

#1 0x000041802a151e01 in Heap_Free (heap=0x43238f2c9000, mem=<optimized out>) at bora/
vmkernel/main/heap.c:4217
```

```
#2 0x000041802a3b0fa1 in BitVector_Free (heap=<optimized out>, bv=<optimized out>) at
bora/vmkernel/util/bitvector.c:94

#3 0x000041802b9f4f3f in HbrBitmapFree (bitmap=<optimized out>) at bora/modules/vmkernel/
hbr_filter/hbr_bitmap.c:91
```

This issue is resolved in this release.

PR 3162499: During service insertion for NSX-managed workload VMs, some VMS might become intermittently unresponsive, and the virtual device might reset

During service insertion for NSX-managed workload VMs, a packet list might be reinjected from the input chain of one switchport to another switchport. In such cases, the source switchport does not correspond to the actual `portID` of the input chain and the virtual device does not get completion status for the transmitted frame. As a result, when you run a service insertion task, some VMs might become intermittently unresponsive due to network connectivity issues.

This issue is resolved in this release.

PR 3219441: You cannot send keys to a guest OS by using the browser console in the ESXi Host Client

In the ESXi Host Client, when you open the browser console of a virtual machine and select **Guest OS > Send keys**, when you select a key input, for example **Ctrl-Alt-Delete**, the selection is not sent to the guest OS.

This issue is resolved in this release.

PR 3209853: Windows VMs might fail with a blue diagnostic screen with 0x5c signature due to platform delays

Windows VMs might fail with a blue diagnostic screen with the following signature due to a combination of factors involving the Windows timer code and platform delays, such as storage or network delays:

`HAL_INITIALIZATION_FAILED (0x5c)` (This indicates that the HAL initialization failed.)

Arguments:

```
Arg1: 0000000000000115, HAL_TIMER_INITIALIZATION_FAILURE

Arg2: fffff7ea800153e0, Timer address

Arg3: 00000000000014da, Delta in QPC units (delta to program the timer with)

Arg4: ffffffffc0000001, invalid status code (STATUS_UNSUCCESSFUL)
```

Checks done by HPET timers in Windows might fail due to such platform delays and cause the issue.

This issue is resolved in this release.

PR 3178109: vSphere Lifecycle Manager compliance check fails with "An unknown error occurred while performing the operation"

The base ESXi image contains driver components that can be overridden by higher version async driver components packaged by an OEM add-on. If such a component is manually removed on a host, the compliance check of the vSphere Lifecycle Manager might fail unexpectedly. In the vSphere Client, you see errors such as `Host status is unknown` and `An unknown error occurred while performing the operation.`

This issue is resolved in this release.

PR 3180634: Performance of certain nested virtual machines on AMD CPUs might degrade

Nested virtual machines on AMD CPUs with operational systems such as Windows with virtualization-based security (VBS) might experience performance degradation, timeouts, or unresponsiveness due to an issue with the virtualization of AMD's Rapid Virtualization Indexing (RVI), also known as Nested Page Tables (NPT).

This issue is resolved in this release.

PR 3223539: Some vmnics might not be visible after an ESXi host reboot due to a faulty NVMe device

If an NVMe device fails during the attach phase, the NVMe driver disables the NVMe controller and resets the hardware queue resources. When you try to re-attach the device, a mismatch between the hardware and driver queue pointers might cause an IOMMU fault on the NVMe device, which leads to memory corruption and failure of the vmkdevmgr service. As a result, you do not see some vmnics in your network.

This issue is resolved in this release.

PR 3218835: When you disable or suspend vSphere Fault Tolerance, virtual machines might become unresponsive for about 10 seconds

When you disable or suspend vSphere FT, some virtual machines might take about 10 seconds to release vSphere FT resources. As a result, such VMs become temporarily unresponsive to network requests or console operations.

This issue is resolved in this release.

PR 3181901: ESXi host becomes unresponsive and you cannot put the host in Maintenance Mode or migrate VMs from that host

Asynchronous reads of metadata on a VMFS volume attached to an ESXi host might cause a race condition with other threads on the host and make the host unresponsive. As a result, you cannot put the host in Maintenance Mode or migrate VMs from that host.

This issue is resolved in this release.

PR 3156666: Packets with length less than 60 bytes might drop

An ESXi host might add invalid bytes, other than zero, to packets with less than 60 bytes. As a result, packets with such invalid bytes drop.

This issue is resolved in this release.

PR 3180283: When you migrate a VM with recently hot-added memory, an ESXi host might repeatedly fail with a purple diagnostic screen

Due to a race condition while the memory hotplug module recomputes the NUMA memory layout of a VM on a destination host after migration, an ESXi host might repeatedly fail with a purple diagnostic screen. In the backtrace, you see errors such as:

```
0x452900262cf0:[0x4200138fee8b]PanicvPanicInt@vmkernel#nover+0x327 stack: 0x452900262dc8,
0x4302f6c06508, 0x4200138fee8b, 0x420013df1300, 0x452900262cf0  0x452900262dc0:
[0x4200138ff43d]Panic_WithBacktrace@vmkernel#nover+0x56 stack: 0x452900262e30,
0x452900262de0, 0x452900262e40, 0x452900262df0, 0x3e7514  0x452900262e30:
[0x4200138fbb90]NMI_Interrupt@vmkernel#nover+0x561 stack: 0x0, 0xf48, 0x0,
0x0, 0x0  0x452900262f00:[0x420013953392]IDTNMIWork@vmkernel#nover+0x7f stack:
0x420049800000, 0x4200139546dd, 0x0, 0x452900262fd0, 0x0  0x452900262f20:
[0x4200139546dc]Int2_NMI@vmkernel#nover+0x19 stack: 0x0, 0x42001394e068,
0xf50, 0xf50, 0x0  0x452900262f40:[0x42001394e067]gate_entry@vmkernel#nover
+0x68 stack: 0x0, 0x43207bc02088, 0xd, 0x0, 0x43207bc02088  0x45397b61bd30:
[0x420013be7514]NUMASched_PageNum2PhysicalDomain@vmkernel#nover+0x58 stack:
0x1, 0x420013be34c3, 0x45396f79f000, 0x1, 0x100005cf757  0x45397b61bd50:
[0x420013be34c2]NUMASched_UpdateAllocStats@vmkernel#nover+0x4b stack: 0x100005cf757, 0x0,
0x0, 0x4200139b36d9, 0x0  0x45397b61bd80:[0x4200139b36d8]VmMem_NodeStatsSub@vmkernel#nover
+0x59 stack: 0x39, 0x45396f79f000, 0xbce0dbf, 0x100005cf757, 0x0  0x45397b61bdc0:
[0x4200139b4372]VmMem_FreePageNoBackmap@vmkernel#nover+0x8b stack: 0x465ec0001be0, 0xa,
0x465ec18748b0, 0x420014e7685f, 0x465ec14437d0
```

This issue is resolved in this release.

PR 3100552: ESXi booting times out after five minutes and the host automatically reboots

During initial ESXi booting, when you see the **Loading VMware ESXi** progress bar, if the bootloader takes more than a total of five minutes to load all the boot modules before moving on to the next phase of booting, the host firmware times out the boot process and resets the system.

This issue is resolved in this release. With ESXi 7.0 Update 3o, the ESXi bootloader resets the five-minute timeout after each boot module loads.

PR 3184368: The durable name of a SCSI LUN might not be set

The durable name property for a SCSI-3 compliant device comes from pages `80h` and `83h` of the Vital Product Data (VPD) as defined by the T10 and SMI standards. To populate the durable name, ESXi first sends an inquiry command to get a list of VPD pages supported by the device. Then ESXi issues commands to get data for all supported VPD pages. Due to an issue with the target array, the device might fail a command to get VPD page data for a page in the list with a `not supported` error. As a result, ESXi cannot populate the durable name property for the device.

This issue is resolved in this release. The fix ignores the error on command to get VPD page data, except pages `80h` and `83h` , if that data is not required for the generation of durable name.

PR 3184425: Port scan of a VXLAN Tunnel End Point (VTEP) on an ESXi host might result in an intermittent connectivity loss

Port scan of a VTEP on an ESXi host might result in an intermittent connectivity loss, but only under the following conditions:

1. Your environment has many VTEPs
2. All VTEPs are in the same IP subnet
3. The upstream switch is Cisco ACI

This issue is resolved in this release.

PR 3156627: Changing the mode of the virtual disk on a running virtual machine might cause the VM to fail

If you use the VMware Host Client to edit the disk mode of a running virtual machine, for example from Independent - Nonpersistent to Dependent or Independent - Persistent, the operation fails and might cause the VM to fail. In the `vmware.log` , you see errors such as:

```
msg.disk.notConfigured2] Failed to configure disk 'scsi0:4'. The virtual machine cannot be powered on with an unconfigured disk.
```

```
[msg.checkpoint.continuesync.error] An operation required the virtual machine to quiesce and the virtual machine was unable to continue running.
```

This issue is resolved in this release. The fix blocks changing the mode of an Independent - Nonpersistent disk on a running virtual machine by using the VMware Host Client. The vSphere Client already blocks such operations.

PR 3164477: In VMware Skyline Health Diagnostics, you see multiple warnings for vSAN memory pools

The free heap memory estimation logic for some vSAN memory pools might consider more memory heap than actual and trigger warnings for insufficient memory. As a result, you see `Memory pools (heap)` health warnings for many hosts under the **Physical disks** section in Skyline Health.

This issue is resolved in this release.

PR 3168950: ESXi hosts fail with a purple diagnostic screen while installing VMware NSX-T Data Center due to insufficient TCP/IP heap space

VMware NSX-T Data Center has multiple net stacks and the default TCP/IP heap space might not be sufficient for installation. As a result, ESXi hosts might fail with a purple diagnostic screen.

This issue is resolved in this release. The fix increases the default `TcpipHeapSize` setting to 8 MB from 0 MB and the maximum size to 128 MB from 32 MB. In the vSphere Client, you can change the `TcpipHeapSize` value by navigating to

Hosts and Clusters > Configure > System > Advanced System Settings > TcpipHeapSize. In vCenter systems with VMware NSX-T Data Center, set the value to 128 MB.

PR 3096974: Rare race condition in I/O filters might cause an ESXi host to fail with a purple diagnostics screen

ESXi hosts in which virtual machines use I/O filters might randomly fail with a purple diagnostics screen and an error such as `#DF Exception 8 IP 0x42002c54b19f SP 0x453a9e8c2000` due to a rare race condition.

This issue is resolved in this release.

PR 3112194: Spherelet might fail to start on an ESXi host due to the execInstalledOnly setting

The `execInstalledOnly` setting is a run time parameter which limits execution of binaries such as applications and vmkernel modules to improve security and guard against breaches and compromises. Some `execInstalledOnly` security checks might interfere with Spherelet, the ESXi UserWorld agent that acts as an extension to the Kubernetes Control Plane, and prevent it to start, even when all files are installed.

This issue is resolved in this release.

PR 3115870: VMware VIB installation might fail during concurrent vendor package installations

When you install update packages from several vendors, such as JetStream Software, Microsoft, and VMware, multiple clients call the same PatchManager APIs and might lead to a race condition. As a result, VMware installation packages (VIBs) might fail to install. In the logs, you see an error such as `vim.fault.PlatformConfigFault` , which is a catch-all fault indicating that some error has occurred regarding the configuration of the ESXi host. In the vSphere Client, you see a message such as `An error occurred during host configuration.`

This issue is resolved in this release. The fix is to return a `TaskInProgress` warning instead of `PlatformConfigFault` , so that you are aware of the actual issue and retry the installation.

PR 3164439: Certain applications might take too many ESXi file handles and cause performance aggravation

In very rare cases, applications such as NVIDIA virtual GPU (vGPU) might consume so many file handles that ESXi fails to process other services or VMs. As a result, you might see GPU on some nodes to disappear, or report zero GPU memory, or performance degradation.

This issue is resolved in this release. The fix reduces the number of file handles a vGPU VM can consume.

PR 3162963: If parallel volume expand and volume refresh operations on the same VMFS volume run on two ESXi hosts in the same cluster, the VMFS volume might go offline

While a VMFS volume expand operation is in progress on an ESXi host in a vCenter cluster, if on another host a user or vCenter initiates a refresh of the same VMFS volume capacity, such a volume might go offline. The issue occurs due to a possible mismatch in the device size, which is stamped on the disk in the volume metadata during a device rescan, and the device size value in the Pluggable Storage Architecture (PSA) layer on the host, which might not be updated if the device rescan is not complete.

This issue is resolved in this release. The fix improves the resiliency of the volume manager code to force a consecutive refresh of the device attributes and comparison of the device sizes again if vCenter reports a mismatch in the device size.

PR 3161690: CPU usage of ESXi hosts might intermittently increase in environments

Due to a rare race condition, when a VM power off command conflicts with a callback function, you might see increased CPU usage on ESXi hosts, for example, after an upgrade.

This issue is resolved in this release.

PR 3165374: ESXi hosts might become unresponsive and fail with a purple diagnostic screen during TCP TIME_WAIT

The TCP slow timer might starve TCP input processing while it covers the list of connections in `TIME_WAIT` closing expired connections due to contention on the global TCP pcbinfo lock. As a result, the VMkernel might fail with a purple

diagnostic screen and the error `Spin count exceeded - possible deadlock` while cleaning up `TCP TIME_WAIT` sockets. The backtrace points to tcpip functions such as `tcp_slowtimo()` or `tcp_twstart()`.

This issue is resolved in this release. The fix adds a new global lock to protect the list of connections in `TIME_WAIT` and to acquire the TCP pcbinfo lock only when closing an expired connection.

PR 3166818: If any of the mount points that use the same NFS server IP returns an error, VAAI-NAS might mark all mount points as not supported

When you use a VAAI-NAS vendor plug-in, multiple file systems on an ESXi host use the same NFS server IP to create a datastore. For certain NAS providers, if one of the mounts returns a `VIX_E_OBJECT_NOT_FOUND (25)` error during the `startSession` call, hardware acceleration for all file systems with the same NFS server IP might become unsupported. This issue occurs when an ESXi host mounts a directory on an NFS server, but that directory is not available at the time of the `startSession` call, because, for example, it has been moved from that NFS server.

This issue is resolved in this release. The fix makes sure that VAAI-NAS marks as not supported only mounts that report an error.

PR 3100030: An ESXi host fails with a purple diagnostic screen indicating VMFS heap corruption

A race condition in the host cache of a VMFS datastore might cause heap corruption and the ESXi host fails with a purple diagnostic screen and a message such as:

```
PF Exception 14 in world xxxxx:res3HelperQu IP 0xxxxxxe2 addr 0xXXXXXXXXX
```

This issue is resolved in this release.

PR 3121216: If the Internet Control Message Protocol (ICMPA) is not active, ESXi host reboot might take long after an upgrade

If ICMPA is not active on the NFS servers in your environment, after upgrading your system, ESXi hosts reboot might take an hour to complete, because restore operations for NFS datastores fail. NFS uses the `vmkping` utility to identify reachable IPs of the NFS servers before executing a mount operation and when ICMP is not active, mount operations fail.

This issue is resolved in this release. To remove dependency on the ICMP protocol to find reachable IPs, the fix adds socket APIs to ensure that IPs on a given NFS server are available.

PR 3098760: ESXi hosts randomly disconnect from the Active Directory domain or vCenter due to Likewise memory exhaustion

Memory leaks in Active Directory operations and related libraries, or when smart card authentication is enabled on an ESXi host, might lead to Likewise memory exhaustion.

This issue is partially resolved in this release. For more information, see VMware knowledge base article 78968.

PR 3118402: The NTP monitoring function returns intermittent time sync failure in the time services test report even when the ESXi host system clock is actually in sync

The time services monitoring infrastructure periodically queries the NTP daemon, ntpd, for time sync status on ESXi hosts. Intermittent query failures might occur due to timeouts in the socket call to read such status information. As a result, you might see time sync failure alerts in the NTP test reports.

This issue is resolved in this release. The fix makes sure that NTP monitoring queries do not fail.

PR 3159168: You see multiple "End path evaluation for device" messages in the vmkernel.log

A periodic device probe that evaluates the state of all the paths to a device might create multiple unnecessary `End path evaluation for device` messages in the `vmkernel.log` file on a release build.

This issue is resolved in this release. The fix restricts `End path evaluation for device` messages to only non-release builds, such as beta. You must enable the VERBOSE log level to see such logs.

PR 3101512: You see a warning for lost uplink redundancy even when the uplink is active

If you quickly remove the network cable from a physical NIC and reinsert it, the ESXi host agent, hostd, triggers an event to restore uplink redundancy, but in some cases, although the uplink restores in a second, you still see a misleading alarm for lost uplink redundancy.

This issue is resolved in this release.

PR 3161473: Operations with stateless ESXi hosts might not pick the expected remote disk for system cache, which causes remediation or compliance issues

Operations with stateless ESXi hosts, such as storage migration, might not pick the expected remote disk for system cache. For example, you want to keep the new boot LUN as LUN 0, but vSphere Auto Deploy picks LUN 1.

This issue is resolved in this release. The fix provides a consistent way to sort the remote disks and always pick the disk with the lowest LUN ID. To make sure you enable the fix, follow these steps:

1. On the Edit host profile page of the Auto Deploy wizard, select **Advanced Configuration Settings** > **SystemImage Cache Configuration** > **System Image Cache Configuration**
2. In the **System Image Cache Profile Settings** drop-down menu, select **Enable stateless caching on the host**.
3. Edit **Arguments** for first disk by replacing **remote** with **sortedremote** and/or **remoteesx** with **sortedremoteesx**.

PR 3187846: Setting the screen resolution of a powered off, encrypted virtual machine does not always work when manually editing the VMX file

If you manually specify the screen resolution of a powered off, encrypted virtual machine by editing the VMX file, the change might not take effect.

This issue is resolved in this release.

esx-update_7.0.3-0.105.22348816

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.105.22348816 • VMware_bootbank_esx-update_7.0.3-0.105.22348816
PRs Fixed	3245953, 3178109, 3211395, 3164477, 3119959, 3164462
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

Broadcom-lsi-msgpt3_17.00.12.00-2vmw.703.0.105.22348816

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A

Affected VIBs	• VMW_bootbank_lsi-msgpt3_17.00.12.00-2vmw.703.0.105.22348816
PRs Fixed	3036883
CVE numbers	N/A

Updates the `ntg3` VIB to resolve the following issue:

PR 3036883: A SAS path might be lost during upgrade of lsi_msgpt3 drivers

Upgrading `lsi_msgpt3` drivers of version `17.00.12.00-1` and earlier might cause storage connections and VMs on ESXi host to become unresponsive due to a lost SAS path. In the VMkernel logs, you see error messages such as:

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: NMP: nmpDeviceAttemptFailover:640:
Retry world failover device "naa.6000d310045e2c000000000000000043" - issuing command
0x459acc1f5dc0
```

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: vmw_psp_rr: psp_rrSelectPath:2177: Could
not select path for device "naa.6000d310045e2c000000000000000043".
```

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: NMP: nmpDeviceAttemptFailover:715: Retry
world failover device "naa.6000d310045e2c000000000000000043" - failed to issue command due
to Not found (APD), try again...
```

This issue is resolved in this release. If you already face the issue, rescan your storage after failing back on storage controller to recover the paths and storage connections.

Microchip-smartpqiv2-plugin_1.0.0-9vmw.703.0.105.22348816

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_lsuv2-smartpqiv2-plugin_1.0.0-9vmw.703.0.105.22348816
PRs Fixed	3112692
CVE numbers	N/A

Updates the `lsuv2-smartpqiv2-plugin` VIB to resolve the following issue:

PR 3112692: The smartpqi driver cannot get the location of ThinkSystem PM1645a SAS SSD devices

In rare cases, the `smartpqi plugin in LSU service` might get a longer serial number string from the VPD page 0x80 than the actual serial number, and the device lookup in the cache fails. As a result, when you run the command `esxcli storage core device physical get -d <device_id>` to get a device location, you see an error such as `Unable to get location for device. Device is not found.`.

This issue is resolved in this release. The fix makes sure that the `smartpqi plugin in LSU service` always checks the correct serial number length and finds the device location.

VMware-NVMe-PCIe_1.2.3.16-3vmw.703.0.105.22348816

Patch Category	Bugfix

Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_nvme-pcie_1.2.3.16-3vmw.703.0.105.22348816
PRs Fixed	3218578
CVE numbers	N/A

Updates the `nvme-pcie` VIB to resolve the following issue:

PR 3218578: You see wrong device descriptions of some Lenovo ThinkSystem boot RAID adapters

In a vSphere client interface, such as the vSphere Client, or when you run commands such as `lspci` and `esxcfg-scsidevs -a` from the ESXi shell, you might see the device names of some Lenovo-branded boot SATA/NVMe adapters as the generical names of the controller chips they use. For example, **Lenovo ThinkSystem M.2 with Mirroring Enablement Kit** is displayed as **88SE9230 PCIe SATA 6GB/s controller**.

This issue is resolved in this release.

VMware-ahci_2.0.11-2vmw.703.0.105.22348816

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_vmw-ahci_2.0.11-2vmw.703.0.105.22348816
PRs Fixed	3218578
CVE numbers	N/A

Updates the `vmw-ahci` VIB.

Intel-Volume-Mgmt-Device_2.7.0.1157-3vmw.703.0.105.22348816

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_iavmd_2.7.0.1157-3vmw.703.0.105.22348816
PRs Fixed	3224847
CVE numbers	N/A

Updates the `iavmd` VIB.

ESXi_7.0.3-0.100.22348808

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vsanhealth_7.0.3-0.100.22348808 • VMware_bootbank_crx_7.0.3-0.100.22348808 • VMware_bootbank_vdfs_7.0.3-0.100.22348808 • VMware_bootbank_esxio-combiner_7.0.3-0.100.22348808 • VMware_bootbank_native-misc-drivers_7.0.3-0.100.22348808 • VMware_bootbank_esx-base_7.0.3-0.100.22348808 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.100.22348808 • VMware_bootbank_cpu-microcode_7.0.3-0.100.22348808 • VMware_bootbank_bmcal_7.0.3-0.100.22348808 • VMware_bootbank_esx-ui_2.11.2-21988676 • VMware_bootbank_gc_7.0.3-0.100.22348808 • VMware_bootbank_trx_7.0.3-0.100.22348808 • VMware_bootbank_vsan_7.0.3-0.100.22348808 • VMware_bootbank_esx-xserver_7.0.3-0.100.22348808
PRs Fixed	3219441, 3239369, 3236018, 3232099, 3232034, 3222887, 3217141, 3213025, 3187868, 3186342, 3164962, 3089785, 3160789, 3098679, 3089785, 3256457
CVE numbers	N/A

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `vsanhealth`, `crx`, `vdfs`, `esxio-combiner`, `native-misc-drivers`, `esx-base`, `esx-dvfilter-generic-fastpath`, `cpu-microcode`, `bmcal`, `esx-ui`, `gc`, `trx`, `vsan`, and `esx-xserver` VIBs to resolve the following issues:

ESXi 7.0 Update 3o provides the following security updates:

- The cURL library is updated to version 8.1.2.
- The ESXi userworld libxml2 library is updated to version 2.10.4.
- The SQLite library is updated to version 3.42.0.
- The OpenSSL package is updated to version 1.0.2zh.

The cpu-microcode VIB includes the following AMD microcode:

Code Name	FMS	MCU Rev	MCU Date	Brand Names
Bulldozer	0x600f12 (15/01/2)	0x0600063e	2/7/2018	Opteron 6200/4200/3200 Series
Piledriver	0x600f20 (15/02/0)	0x06000852	2/6/2018	Opteron 6300/4300/3300 Series

Code Name	FMS	MCU Rev	MCU Date	Brand Names
Zen-Naples	0x800f12 (17/01/2)	0x0800126e	11/11/2021	EPYC 7001 Series
Zen2-Rome	0x830f10 (17/31/0)	0x0830107a	5/17/2023	EPYC 7002/7Fx2/7Hx2 Series
Zen3-Milan-B1	0xa00f11 (19/01/1)	0x0a0011d1	7/10/2023	EPYC 7003/7003X Series
Zen3-Milan-B2	0xa00f12 (19/01/2)	0x0a001234	7/10/2023	EPYC 7003/7003X Series

The cpu-microcode VIB includes the following Intel microcode:

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Westmere EX	0x206f2 (06/2f/2)	0x05	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x4003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x5003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x7002703	3/21/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0xe000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x38	12/2/2021	Intel Atom C3000 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0xd0003a5	3/30/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x1000230	1/27/2023	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	0xac	2/27/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	0x2c	2/27/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	0x46	2/27/2023	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	0x2c0001d1	2/14/2023	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	0x2b000461	3/13/2023	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0xf4	2/23/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0xfa	2/27/2023	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x59	2/26/2023	Intel Xeon E-2300 Series

esx-update_7.0.3-0.100.22348808

Patch Category	Security
Patch Severity	Critical

Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.100.22348808 • VMware_bootbank_esx-update_7.0.3-0.100.22348808
PRs Fixed	N/A
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

VMware-VM-Tools_12.2.6.22229486-22348808

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_locker_tools-light_12.2.6.22229486-22348808
PRs Fixed	3178522, 3178519
CVE numbers	N/A

Updates the `tools-light` VIB.

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3o:

- **windows.iso**: VMware Tools 12.2.6 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
- **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. For more details, see VMware knowledge base article 88698.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- Updating VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- What Every vSphere Admin Must Know About VMware Tools
- Earlier versions of VMware Tools
- VMware Tools 12.2.6 Release Notes

ESXi-7.0U3o-22348816-standard

Profile Name	ESXi-7.0U3o-22348816-standard
Build	For build information, see Patches Contained in This Release.
Vendor	VMware, Inc.
Release Date	September 28, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.105.22348816 • VMware_bootbank_native-misc-drivers_7.0.3-0.105.22348816 • VMware_bootbank_vsanhealth_7.0.3-0.105.22348816 • VMware_bootbank_crx_7.0.3-0.105.22348816 • VMware_bootbank_esx-xserver_7.0.3-0.105.22348816 • VMware_bootbank_vdfs_7.0.3-0.105.22348816 • VMware_bootbank_cpu-microcode_7.0.3-0.105.22348816 • VMware_bootbank_esx-base_7.0.3-0.105.22348816 • VMware_bootbank_vsan_7.0.3-0.105.22348816 • VMware_bootbank_esxio-combiner_7.0.3-0.105.22348816 • VMware_bootbank_esx-ui_2.11.2-21988676 • VMware_bootbank_bmcal_7.0.3-0.105.22348816 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.105.22348816 • Mware_bootbank_trx_7.0.3-0.105.22348816 • VMware_bootbank_loadesx_7.0.3-0.105.22348816 • VMware_bootbank_esx-update_7.0.3-0.105.22348816 • VMW_bootbank_lsi-msgpt3_17.00.12.00-2vmw.703.0.105.22348816 • VMware_bootbank_lsuv2-smartpqiv2-plugin_1.0.0-9vmw.703.0.105.22348816 • VMW_bootbank_nvme-pcie_1.2.3.16-3vmw.703.0.105.22348816 • VMW_bootbank_vmw-ahci_2.0.11-2vmw.703.0.105.22348816 • VMW_bootbank_iavmd_2.7.0.1157-3vmw.703.0.105.22348816 • VMware_locker_tools-light_12.2.6.22229486-22233486
PRs Fixed	3244098, 3216958, 3245763, 3242021, 3246132, 3253205, 3256804, 3239170, 3251981, 3215370, 3117615, 3248478, 3252676, 3235496, 3238026, 3236064, 3224739, 3224306, 3223755, 3216958, 3233958, 3185125, 3219264, 3221620, 3218835, 3185560, 3221099, 3211625, 3221860, 3228586, 3224604, 3223539, 3222601, 3217258, 3213041, 3216522, 3221591, 3216389, 3220004, 3217633, 3216548, 3216449, 3156666, 3181574, 3180746, 3155476, 3211807, 3154090, 3184008, 3183519, 3183519, 3209853, 3100552, 3187846, 3113263, 3176350, 3185827, 3095511, 3184425, 3186351, 3186367, 3154090, 3158524, 3181601, 3180391, 3180283, 3184608, 3181774, 3155476, 3163361, 3182978, 3184368, 3160456, 3164575, 3181901, 3184871, 3166818, 3157195, 3164355, 3163271, 3112194, 3161690, 3261925, 3178589, 3178721, 3162963, 3168950, 3159168, 3158491, 3158866, 3096769, 3165374, 3122037, 3098760, 3164439, 3161473,

	3162790, 3100030, 3096974, 3161473, 3165651, 3083007, 3118240, 3151076, 3118402, 3160480, 3156627, 3158531, 3162499, 3158512, 3053430, 3153395, 3117615, 3099192, 3158508, 3115870, 3119834, 3158220, 3110401, 2625439, 3099357, 3152811, 3108979, 3120165, 3245953, 3178109, 3211395, 3164477, 3119959, 3164462, 3036883, 3112692, 3218578, 3224847
Related CVE numbers	N/A

This patch updates the following issues:

PR 3187846: Setting the screen resolution of a powered off, encrypted virtual machine does not always work when manually editing the VMX file

If you manually specify the screen resolution of a powered off, encrypted virtual machine by editing the VMX file, the change might not take effect.

This issue is resolved in this release.

PR 3253205: Static IPv6 gateway disappears in 18 hours

If you configure a static IPv6 gateway address in your vSphere environment, such gateways might no longer exist in up to 18 hours due to a timeout.

This issue is resolved in this release. The fix removes the existing timeout for static gateways.

PR 3272532: You see speed as Half Duplex after changing the speed from Auto to Full on a VMNIC

In some cases, length checks during the parsing of duplex TLVs in an environment with active Cisco Discovery Protocol (CDP) might fail. As a result, when you change the speed from **Auto** to **Full** on a physical NIC on peer devices you do not see the real duplex value in the TLV under the neighbor information, but the default Half Duplex value.

This issue is resolved in this release.

PR 3251981: An NFSv4.1 file might appear to be empty even though it contains data

When you open an existing NFSv4.1 file with write only access, if for some reason the NFS client opens again the same file with read only access, read operations from the client might return no data although the file is not empty.

This issue is resolved in this release.

PR 3116601: When you override the default gateway for the vSAN VMkernel adapter on an ESXi host, the vSphere HA agent on the host displays as inaccessible

In some cases, when you override the default gateway for the vSAN VMkernel adapter on an ESXi host, the Fault Domain Manager (FDM), which is the agent that vSphere HA deploys on ESX hosts, might stop receiving Internet Control Message Protocol (ICMP) pings. As a result, FDM might issue false cluster alarms that the vSphere HA agent on the host cannot reach some management network addresses of other hosts.

This issue is resolved in this release.

PR 3251801: vSphere vMotion operation from a 6.7.x ESXi host with an Intel Ice Lake CPU fails with msg.checkpoint.cpucheck.fail

vSphere vMotion operations by using either the vSphere Client or VMware Hybrid Cloud Extension (HCX) from an Intel Ice Lake CPU host running ESXi 6.7.x fails with an error such as `msg.checkpoint.cpucheck.fail` . In the vSphere Client, you see a message that cpuid.PSFD is not supported on the target host. In HCX, you see a report such as `A general system error occurred: vMotion failed:` .

This issue is resolved in this release.

PR 3036883: A SAS path might be lost during upgrade of lsi_msgpt3 drivers

Upgrading `lsi_msgpt3` drivers of version `17.00.12.00-1` and earlier might cause storage connections and VMs on ESXi host to become unresponsive due to a lost SAS path. In the VMkernel logs, you see error messages such as:

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: NMP: nmpDeviceAttemptFailover:640:
Retry world failover device "naa.6000d310045e2c000000000000000043" - issuing command
0x459acc1f5dc0
```

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: vmw_psp_rr: psp_rrSelectPath:2177: Could
not select path for device "naa.6000d310045e2c000000000000000043".
```

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: NMP: nmpDeviceAttemptFailover:715: Retry
world failover device "naa.6000d310045e2c000000000000000043" - failed to issue command due
to Not found (APD), try again...
```

This issue is resolved in this release. If you already face the issue, rescan your storage after failing back on storage controller to recover the paths and storage connections.

PR 3224739: You see alarms for dropped syslog messages

If the network throughput of your vSphere system does not align with the speed at which log messages are generated, some of the log messages sent to the remote syslog server might drop. As a result, in the vSphere Client you see host errors of type `Triggered Alarm` and in the logs, you see warnings such as `ALERT: vmsyslog logger xxxx:514 lost yyyy log messages.`

This issue is resolved in this release. The fix improves the network logging performance of the logging service to reduce the number of such lost log messages.

PR 3247027: If any failure occurs during a vSphere vMotion migration of NVIDIA virtual GPU (vGPU) VM, the destination ESXi host might fail with a purple diagnostic screen

In very rare cases, if any type of failure occurs during a vSphere vMotion migration of a vGPU VM, the vMotion operation is marked as a failure while a specific internal operation is in progress. As a result, the destination ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3095511: The SFCB service intermittently fails and generates "sfcb-vmware_bas-zdump" files on multiple ESXi hosts

In very rare cases, when the SFCB service tries to access an uninitialized variable, the service might fail with dump file such as `sfcb-vmware_bas-zdump.000`. The issue occurs because accessing an uninitialized variable can cause the SFCB process to keep requesting memory until it exceeds the heap allocation.

This issue is resolved in this release.

PR 3218578: You see wrong device descriptions of some Lenovo ThinkSystem boot RAID adapters

In a vSphere client interface, such as the vSphere Client, or when you run commands such as `lspci` and `esxcfg-scsidevs -a` from the ESXi shell, you might see the device names of some Lenovo-branded boot SATA/NVMe adapters as the generical names of the controller chips they use. For example, **Lenovo ThinkSystem M.2 with Mirroring Enablement Kit** is displayed as **88SE9230 PCIe SATA 6GB/s controller**.

This issue is resolved in this release.

PR 3256804: File server loses connectivity after failover when running vSAN File Service on NSX overlay network

If vSAN File Service is running on an NSX overlay network, the file server might lose connectivity after it fails over from one agent VM to another agent VM. The file server can failover when reconfiguring file service domain from such without Active Directory(AD) to such with AD, or if vSAN detects unhealthy behavior in the file server, file share, or AD server. If file server connectivity is lost after a failover, File Service clients cannot access the file share. The following health warning might be reported:

`One or more DNS servers is not reachable.`

This issue is resolved in this release.

PR 3217633: vSAN management service on the orchestration host malfunctions during vCenter restart

This issue can occur on vSAN clusters where vCenter is deployed. If multiple cluster shutdown operations are performed, the `/etc/vmware/vsan/vsanperf.conf` file on the orchestration host can contain two versions of the following management VM: `vc_vm_moIdvc_vm_moid` . These configuration options conflict with each other and can cause the vSAN management service to malfunction.

This issue is resolved in this release.

PR 3224306: When you change the ESXi syslog setting syslog.global.logDir, if syslog.global.logDirUnique is active, you might see 2 levels of <hostname> subdir under the logdir path

After upgrading an ESXi host to 7.0 Update 3c and later, if you change the syslog setting `syslog.global.logDir` and the `syslog.global.logDirUnique` setting is active, you might see 2 levels of `<hostname>` subdirs under the `logdir` path on the host. The `syslog.global.logDirUnique` setting is useful if the same NFS directory is configured as the `Syslog.global.LogDir` by multiple ESXi hosts, as it creates a subdirectory with the name of the ESXi host under `logdir` .

This issue is resolved in this release.

PR 3223755: ESXi syslog daemon fails to resume transmitting logs to the configured SSL remote syslog server once a drop in the network connectivity restores

If a remote SSL syslog server temporarily loses connectivity, the ESXi syslog daemon might fail to resume transmitting logs after connectivity restores and you must restart the service to re-activate transmissions. The issue occurs due to some unhandled exceptions while the ESXi syslog daemon tries to restore connection to the SSL remote syslog server.

This issue is resolved in this release. The fix adds a generic catch for all unhandled exceptions.

PR 3185536: vSAN cluster remediation error after vCenter upgrade to 7.0 Update 3

When you upgrade vCenter from version 6.5.x to 7.0 Update 3, and reconfigure the vSAN cluster, a vSAN cluster remediation is triggered, but in some cases fails.

This issue is resolved in this release.

PR 3110401: The Explicit Congestion Notification (ECN) setting is not persistent on ESXi host reboot

ECN, specified in RFC 3168, allows a TCP sender to reduce the transmission rate to avoid packet drops and is activated by default. However, if you change the default setting, or manually deactivate ECN, such changes to the ESXi configuration might not persist after a reboot of the host.

This issue is resolved in this release.

PR 3153395: Upon refresh, some dynamic firewalls rules might not persist and lead to vSAN iSCSI Target service failure

If you frequently run the command `esxcli network firewall refresh` , a race condition might cause some dynamic firewalls rules to be removed upon refresh or load. As a result, some services such as the vSAN iSCSI Target daemon, which provides vSAN storage with iSCSI protocol, might fail.

This issue is resolved in this release.

PR 3096769: You see high latency for VM I/O operations in a vSAN cluster with Unmap activated

This issue affects vSAN clusters with Unmap activated. A problem in Unmap handling in LSOM creates log congestion. The log congestion can cause high VM I/O latency.

This issue is resolved in this release.

PR 3163361: The Audit Record Storage Capacity parameter does not persist across ESXi host reboots

After an ESXi host reboot, you see the **Audit Record Storage Capacity** parameter restored to the default value of 4 MiB, regardless of any previous changes.

This issue is resolved in this release.

PR 3162496: If the Internet Control Message Protocol (ICMPA) is not active, ESXi host reboot might take long after upgrading to vSphere 8.0 and later

If ICMPA is not active on the NFS servers in your environment, after upgrading your system to vSphere 8.0 and later, ESXi hosts reboot might take an hour to complete, because restore operations for NFS datastores fail. NFS uses the `vmkping` utility to identify reachable IPs of the NFS servers before executing a mount operation and when ICMP is not active, mount operations fail.

This issue is resolved in this release. To remove dependency on the ICMP protocol to find reachable IPs, the fix adds socket APIs to ensure that IPs on a given NFS server are available.

PR 3220004: VBS-enabled Windows VMs might fail with a blue diagnostic screen when an ESXi host is under memory pressure

Windows VMs with virtualization-based security (VBS) enabled might intermittently fail with a blue diagnostic screen during memory-heavy operations such as deleting snapshots or consolidating disks. The BSOD has the following signature:

```
DRIVER_VERIFIER_DMA_VIOLATION (e6)
An illegal DMA operation was attempted by a driver being verified.
```

Arguments:

```
Arg1: 0000000000000026, IOMMU detected DMA violation.
Arg2: 0000000000000000, Device Object of faulting device.
Arg3: xxxxxxxxxxxxxxxx, Faulting information (usually faulting physical address).
Arg4: 0000000000000008, Fault type (hardware specific).
```

This issue is resolved in this release.

PR 3162905: ESXi hosts might intermittently disconnect from vCenter in case of memory outage

In rare cases, if vCenter fails to allocate or transfer active bitmaps due to an alert for insufficient memory for any reason, the hostd service might repeatedly fail and you cannot reconnect the host to the vCenter.

This issue is resolved in this release. The fix makes sure that in such cases you see an error rather than the hostd service failure.

PR 3108979: Staging ESXi patches and ESXi upgrade tasks might become indefinitely unresponsive due to a log buffer limit

If a large string or log exceed the python log buffer limit of 16K, the logger becomes unresponsive. As a result, when you stage ESXi patches on a host by using the vSphere Client, the process responsible for completing the staging task on ESXi might become indefinitely unresponsive. The task times out and reports an error. The issue occurs also when you remediate ESXi hosts by using a patch baseline.

This issue is resolved in this release. The fix breaks the large input string into smaller chunks for logging.

PR 3219264: vSAN precheck for maintenance mode or disk decommission doesn't list objects that might lose accessibility

This issue affects objects with resyncing components, and some components reside on a device to be removed or placed into maintenance mode. When you run a precheck with the **No-Action** option, the precheck does not evaluate the object correctly to report it in the `inaccessibleObjects` list.

This issue is resolved in this release. Precheck includes all affected objects in the `inaccessibleObjects` list.

PR 3186545: Vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable

Some third-party tools for vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable.

This issue is resolved in this release.

PR 3221591: ESXi NVMe/TCP initiator fails to recover paths after target failure recovery

When a NVMe/TCP target recovers from a failure, ESXi cannot recover the path.

This issue is resolved in this release.

PR 3186351: You see an override flag of NIC teaming, security, or traffic shaping policy on a portgroup unexpectedly enabled post an ESXi host reboot

In some cases, a networking configuration might not persist in the ESXi ConfigStore and you see an override flag of NIC teaming, security, or traffic shaping policy on a portgroup unexpectedly enabled post an ESXi host reboot.

This issue is resolved in this release.

PR 3162790: The sfcb daemon might fail with a core dump while installing a third-party CIM provider

The sfcb daemon might try to access already freed memory when registering a CIM provider and fail with a core dump while installing a third-party CIM provider, such as Dell OpenManage Server Administrator for example.

This issue is resolved in this release.

PR 3157195: ESX hosts might fail with a purple diagnostic screen and an error NMI IPI: Panic requested by another PCPU

The resource pool cache is a VMFS specific volume level cache that stores the resource clusters corresponding to the VMFS volume. While searching for priority clusters, the cache flusher workflow iterates through a large list of cached resource clusters, which can cause lockup of the physical CPUs. As a result, ESX hosts might fail with a purple diagnostic screen. In the `logDump` file, you see an error such as:

```
^[[7m2022-10-22T07:56:47.322Z cpu13:2101160)WARNING: Heartbeat: 827: PCPU 0 didn't have a heartbeat for 7 seconds, timeout is 14, 1 IPIs sent; *may* be locked up.^[[0m^
[[31;1m2022-10-22T07:56:47.322Z cpu0:2110633)ALERT: NMI: 710: NMI IPI: RIPOFF(base):RBP:CS
```

This issue is resolved in this release.

PR 3230493: If a delta sync runs while the target vSphere Replication server is not active, Windows virtual machines might become unresponsive

If the target Sphere Replication server is not active during a delta sync, the synchronization process cannot complete and Windows virtual machines become unresponsive.

This issue is resolved in this release. The fix makes sure that no delta sync jobs start when a Sphere Replication server is not active.

PR 3122037: ESXi ConfigStore database fills up and writes fail

Stale data related to block devices might not be deleted in time from the ESXi ConfigStore database and cause an out of space condition. As a result, write operations to ConfigStore start to fail. In the backtrace, you see logs such as:

`2022-12-19T03:51:42.733Z cpu53:26745174)WARNING: VisorFSRam: 203: Cannot extend visorfs file /etc/vmware/configstore/current-store-1-journal because its ramdisk (configstore) is full .`

This issue is resolved in this release.

PR 3246132: You see a system clock drift on an ESXi host after synchronization with the NTP server fails

If connectivity between the NTP server and an ESXi host is delayed for some reason, the system clock on the ESXi host might experience a drift. When you run the `vsish` command `vsish -e get /system/ntpclock/clockData` , you might see a large negative value for the `adjtime` field. For example:

```
NTP clock data {
...  adjtime() (usec):-309237290312 <<<<<<
...
}
```

This issue is resolved in this release.

PR 3185560: vSphere vMotion operations for virtual machines with swap files on a vSphere Virtual Volumes datastore intermittently fail after a hot extend of the VM disk

vSphere vMotion operations for virtual machines with swap files on a vSphere Virtual Volumes datastore might fail under the following circumstances:

A VM that runs on ESXi host A is migrated to ESXi host B, then the VM disk is hot extended, and the VM is migrated back to ESXi host A. The issue occurs due to stale statistics about the swap virtual volume.

This issue is resolved in this release.

PR 3236207: You cannot unmount an NFS v3 datastore from a vCenter system because the datastore displays as inaccessible

While unmounting an NFSv3 datastore from a vCenter system by using either the vSphere Client or ESXCLI, you might see the datastore either as inaccessible, or get an `Unable to Refresh` error. The issue occurs when a hostd cache refresh happens before NFS deletes the mount details from ConfigStore, which creates a rare race condition.

This issue is resolved in this release.

PR 3236064: Compliance or remediation scans by using vSphere Lifecycle Manager might take long on ESXi hosts with a large number of datastores

Compliance or remediation scans by using vSphere Lifecycle Manager include an upgrade precheck that lists all volumes attached to an ESXi host, their free space, versions, and other details. If a host has many datastores attached, each with a large capacity, the precheck can take long. The time is multiplied by the number of baselines attached to the cluster or host.

This issue is resolved in this release. If you already face the issue, disconnect the attached datastores while performing the remediation or compliance scans and reattach them after the operations complete.

PR 3245763: During a vSphere vMotion operation, destination ESXi hosts with a Distributed Firewall (DFW) enabled might fail with a purple diagnostic screen

If the destination host in a vSphere vMotion operation has a DFW enabled, a rare race condition might cause the host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3158866: Virtual machines might become unresponsive during VMFS volume expansion due to a Logical Volume Manager (LVM) check

If a VMFS volume expansion operation happens during a LVM probe to update volume attributes, such as the size of the VMFS partition backing of the VMFS volume, the current size of the VMFS volume might not match the LVM metadata on the disk. As a result, LVM marks such a volume offline and virtual machines on that volume become unresponsive.

This issue is resolved in this release. The fix improves Input Output Control (IOCTL) to speed up the update of device attributes and avoid such cases.

PR 3152717: vSphere Auto Deploy workflows might fail after an upgrade to vCenter Server 7.0 Update 3j or later

Due to a networking issue in reverse proxy configuration environments, vSphere Auto Deploy workflows might fail after an upgrade to vCenter Server 7.0 Update 3j or later. In the ESXi management console and in the `/var/log/vmware/rbd/rbd-cgi.log file` you see an HTTP client error.

This issue is resolved in this release. The fix makes sure Auto Deploy workflows run successfully in reverse proxy configuration environments.

PR 3185125: Virtual SLIT table not populated for the guest OS when using sched.nodeX.affinity

When you specify virtual NUMA node affinity, the vSLIT table might not be populated and you see the following error in `vmware.log : vSLIT: NumaGetLatencyInfo failed with status: 195887107.`

This happens when setting node affinity as follows:

```
numa.slit.enable = "TRUE"

sched.node0.affinity = 0

sched.node1.affinity = 1

...sched.nodeN.affinity = N
```

This issue is resolved in this release. If you already face the issue, specify VCPU affinity to physical CPUs on the associated NUMA nodes, instead of node affinity.

For example:

```
numa.slit.enable = "TRUE"

sched.vcpu0.affinity = "0-7"

sched.vcpu1.affinity = "0-7"

...sched.vcpuN.affinity = "Y-Z"
```

PR 3181774: You do not see an error when you attach a CBT enabled FCD to a VM with CBT disabled

Attaching a First Class Disk (FCD) with Changed Block Tracking (CBT) to a VM with CBT disabled does not throw a detailed error, but the operation cannot take effect. In the backtrace, you might see an error message such as `InvalidState` , which is generic and does not provide details on the issue.

This issue is resolved in this release. The fix adds the error message `Cannot attach a CBT enabled fcd: {path} to CBT disabled VM.` to the logs of the hostd service and adds a status message for the task in the vSphere Client.

PR 3185827: You see trap files in a SNMP directory under /var/spool even though SNMP is not enabled

After the hostd service starts, for example after an ESXi host reboot, it might create a SNMP directory under `/var/spool` and you see many `.trp` files to pile in this directory.

This issue is resolved in this release. The fix makes sure that the directory `/var/spool/snmp` exists only when SNMP is enabled.

PR 3082867: An ESXi host might fail with a purple diagnostic screen after a replicated virtual machine migrates to the host

In some environments, when a replicated virtual machine migrates to a certain ESXi host, during a full sync, some `SCSI WRITE` commands might target address ranges past the end of the transfer map. As a result, the ESXi host might fail with a purple diagnostic screen and a backtrace such as:

```
#0 DLM_free (msp=0x43238f2c9cc0, mem=mem@entry=0x43238f6db860, allowTrim=allowTrim@entry=1
'\001') at bora/vmkernel/main/dlmalloc.c:4924

#1 0x000041802a151e01 in Heap_Free (heap=0x43238f2c9000, mem=<optimized out>) at bora/
vmkernel/main/heap.c:4217

#2 0x000041802a3b0fa1 in BitVector_Free (heap=<optimized out>, bv=<optimized out>) at
bora/vmkernel/util/bitvector.c:94

#3 0x000041802b9f4f3f in HbrBitmapFree (bitmap=<optimized out>) at bora/modules/vmkernel/
hbr_filter/hbr_bitmap.c:91
```

This issue is resolved in this release.

PR 3162499: During service insertion for NSX-managed workload VMs, some VMS might become intermittently unresponsive, and the virtual device might reset

During service insertion for NSX-managed workload VMs, a packet list might be reinjected from the input chain of one switchport to another switchport. In such cases, the source switchport does not correspond to the actual `portID` of the input chain and the virtual device does not get completion status for the transmitted frame. As a result, when you run a service insertion task, some VMs might become intermittently unresponsive due to network connectivity issues.

This issue is resolved in this release.

PR 3219441: You cannot send keys to a guest OS by using the browser console in the ESXi Host Client

In the ESXi Host Client, when you open the browser console of a virtual machine and select **Guest OS > Send keys**, when you select a key input, for example **Ctrl-Alt-Delete**, the selection is not sent to the guest OS.

This issue is resolved in this release.

PR 3209853: Windows VMs might fail with a blue diagnostic screen with 0x5c signature due to platform delays

Windows VMs might fail with a blue diagnostic screen with the following signature due to a combination of factors involving the Windows timer code and platform delays, such as storage or network delays:

`HAL_INITIALIZATION_FAILED (0x5c)` (This indicates that the HAL initialization failed.)

Arguments:

```
Arg1: 0000000000000115, HAL_TIMER_INITIALIZATION_FAILURE

Arg2: fffff7ea800153e0, Timer address

Arg3: 00000000000014da, Delta in QPC units (delta to program the timer with)

Arg4: ffffffffc0000001, invalid status code (STATUS_UNSUCCESSFUL)
```

Checks done by HPET timers in Windows might fail due to such platform delays and cause the issue.

This issue is resolved in this release.

PR 3178109: vSphere Lifecycle Manager compliance check fails with "An unknown error occurred while performing the operation"

The base ESXi image contains driver components that can be overridden by higher version async driver components packaged by an OEM add-on. If such a component is manually removed on a host, the compliance check of the vSphere Lifecycle Manager might fail unexpectedly. In the vSphere Client, you see errors such as `Host status is unknown` and `An unknown error occurred while performing the operation.`

This issue is resolved in this release.

PR 3180634: Performance of certain nested virtual machines on AMD CPUs might degrade

Nested virtual machines on AMD CPUs with operational systems such as Windows with virtualization-based security (VBS) might experience performance degradation, timeouts, or unresponsiveness due to an issue with the virtualization of AMD's Rapid Virtualization Indexing (RVI), also known as Nested Page Tables (NPT).

This issue is resolved in this release.

PR 3223539: Some vmnics might not be visible after an ESXi host reboot due to a faulty NVMe device

If an NVMe device fails during the attach phase, the NVMe driver disables the NVMe controller and resets the hardware queue resources. When you try to re-attach the device, a mismatch between the hardware and driver queue pointers might cause an IOMMU fault on the NVMe device, which leads to memory corruption and failure of the vmkdevmgr service. As a result, you do not see some vmnics in your network.

This issue is resolved in this release.

PR 3218835: When you disable or suspend vSphere Fault Tolerance, virtual machines might become unresponsive for about 10 seconds

When you disable or suspend vSphere FT, some virtual machines might take about 10 seconds to release vSphere FT resources. As a result, such VMs become temporarily unresponsive to network requests or console operations.

This issue is resolved in this release.

PR 3181901: ESXi host becomes unresponsive and you cannot put the host in Maintenance Mode or migrate VMs from that host

Asynchronous reads of metadata on a VMFS volume attached to an ESXi host might cause a race condition with other threads on the host and make the host unresponsive. As a result, you cannot put the host in Maintenance Mode or migrate VMs from that host.

This issue is resolved in this release.

PR 3156666: Packets with length less than 60 bytes might drop

An ESXi host might add invalid bytes, other than zero, to packets with less than 60 bytes. As a result, packets with such invalid bytes drop.

This issue is resolved in this release.

PR 3180283: When you migrate a VM with recently hot-added memory, an ESXi host might repeatedly fail with a purple diagnostic screen

Due to a race condition while the memory hotplug module recomputes the NUMA memory layout of a VM on a destination host after migration, an ESXi host might repeatedly fail with a purple diagnostic screen. In the backtrace, you see errors such as:

```
0x452900262cf0:[0x4200138fee8b]PanicvPanicInt@vmkernel#nover+0x327 stack: 0x452900262dc8,
0x4302f6c06508, 0x4200138fee8b, 0x420013df1300, 0x452900262cf0  0x452900262dc0:
[0x4200138ff43d]Panic_WithBacktrace@vmkernel#nover+0x56 stack: 0x452900262e30,
0x452900262de0, 0x452900262e40, 0x452900262df0, 0x3e7514  0x452900262e30:
[0x4200138fbb90]NMI_Interrupt@vmkernel#nover+0x561 stack: 0x0, 0xf48, 0x0,
0x0, 0x0  0x452900262f00:[0x420013953392]IDTNMIWork@vmkernel#nover+0x7f stack:
0x420049800000, 0x4200139546dd, 0x0, 0x452900262fd0, 0x0  0x452900262f20:
[0x4200139546dc]Int2_NMI@vmkernel#nover+0x19 stack: 0x0, 0x42001394e068,
0xf50, 0xf50, 0x0  0x452900262f40:[0x42001394e067]gate_entry@vmkernel#nover
+0x68 stack: 0x0, 0x43207bc02088, 0xd, 0x0, 0x43207bc02088  0x45397b61bd30:
[0x420013be7514]NUMASched_PageNum2PhysicalDomain@vmkernel#nover+0x58 stack:
0x1, 0x420013be34c3, 0x45396f79f000, 0x1, 0x100005cf757  0x45397b61bd50:
[0x420013be34c2]NUMASched_UpdateAllocStats@vmkernel#nover+0x4b stack: 0x100005cf757, 0x0,
```

```
0x0, 0x4200139b36d9, 0x0  0x45397b61bd80:[0x4200139b36d8]VmMem_NodeStatsSub@vmkernel#nover
+0x59 stack: 0x39, 0x45396f79f000, 0xbce0dbf, 0x100005cf757, 0x0  0x45397b61bdc0:
[0x4200139b4372]VmMem_FreePageNoBackmap@vmkernel#nover+0x8b stack: 0x465ec0001be0, 0xa,
0x465ec18748b0, 0x420014e7685f, 0x465ec14437d0
```

This issue is resolved in this release.

PR 3100552: ESXi booting times out after five minutes and the host automatically reboots

During initial ESXi booting, when you see the **Loading VMware ESXi** progress bar, if the bootloader takes more than a total of five minutes to load all the boot modules before moving on to the next phase of booting, the host firmware times out the boot process and resets the system.

This issue is resolved in this release. With ESXi 7.0 Update 3o, the ESXi bootloader resets the five-minute timeout after each boot module loads.

PR 3184368: The durable name of a SCSI LUN might not be set

The durable name property for a SCSI-3 compliant device comes from pages `80h` and `83h` of the Vital Product Data (VPD) as defined by the T10 and SMI standards. To populate the durable name, ESXi first sends an inquiry command to get a list of VPD pages supported by the device. Then ESXi issues commands to get data for all supported VPD pages. Due to an issue with the target array, the device might fail a command to get VPD page data for a page in the list with a `not supported` error. As a result, ESXi cannot populate the durable name property for the device.

This issue is resolved in this release. The fix ignores the error on command to get VPD page data, except pages `80h` and `83h` , if that data is not required for the generation of durable name.

PR 3184425: Port scan of a VXLAN Tunnel End Point (VTEP) on an ESXi host might result in an intermittent connectivity loss

Port scan of a VTEP on an ESXi host might result in an intermittent connectivity loss, but only under the following conditions:

1. Your environment has many VTEPs
2. All VTEPs are in the same IP subnet
3. The upstream switch is Cisco ACI

This issue is resolved in this release.

PR 3156627: Changing the mode of the virtual disk on a running virtual machine might cause the VM to fail

If you use the VMware Host Client to edit the disk mode of a running virtual machine, for example from Independent - Nonpersistent to Dependent or Independent - Persistent, the operation fails and might cause the VM to fail. In the `vmware.log` , you see errors such as:

```
msg.disk.notConfigured2] Failed to configure disk 'scsi0:4'. The virtual machine cannot be
powered on with an unconfigured disk.
```

```
[msg.checkpoint.continuesync.error] An operation required the virtual machine to quiesce
and the virtual machine was unable to continue running.
```

This issue is resolved in this release. The fix blocks changing the mode of an Independent - Nonpersistent disk on a running virtual machine by using the VMware Host Client. The vSphere Client already blocks such operations.

PR 3164477: In VMware Skyline Health Diagnostics, you see multiple warnings for vSAN memory pools

The free heap memory estimation logic for some vSAN memory pools might consider more memory heap than actual and trigger warnings for insufficient memory. As a result, you see `Memory pools (heap)` health warnings for many hosts under the **Physical disks** section in Skyline Health.

This issue is resolved in this release.

PR 3168950: ESXi hosts fail with a purple diagnostic screen while installing VMware NSX-T Data Center due to insufficient TCP/IP heap space

VMware NSX-T Data Center has multiple net stacks and the default TCP/IP heap space might not be sufficient for installation. As a result, ESXi hosts might fail with a purple diagnostic screen.

This issue is resolved in this release. The fix increases the default `TcpipHeapSize` setting to 8 MB from 0 MB and the maximum size to 128 MB from 32 MB. In the vSphere Client, you can change the `TcpipHeapSize` value by navigating to **Hosts and Clusters > Configure > System > Advanced System Settings > TcpipHeadSize**. In vCenter systems with VMware NSX-T Data Center, set the value to 128 MB.

PR 3096974: Rare race condition in I/O filters might cause an ESXi host to fail with a purple diagnostics screen

ESXi hosts in which virtual machines use I/O filters might randomly fail with a purple diagnostics screen and an error such as `#DF Exception 8 IP 0x42002c54b19f SP 0x453a9e8c2000` due to a rare race condition.

This issue is resolved in this release.

PR 3112194: Spherelet might fail to start on an ESXi host due to the execInstalledOnly setting

The `execInstalledOnly` setting is a run time parameter which limits execution of binaries such as applications and vmkernel modules to improve security and guard against breaches and compromises. Some `execInstalledOnly` security checks might interfere with Spherelet, the ESXi UserWorld agent that acts as an extension to the Kubernetes Control Plane, and prevent it to start, even when all files are installed.

This issue is resolved in this release.

PR 3115870: VMware VIB installation might fail during concurrent vendor package installations

When you install update packages from several vendors, such as JetStream Software, Microsoft, and VMware, multiple clients call the same PatchManager APIs and might lead to a race condition. As a result, VMware installation packages (VIBs) might fail to install. In the logs, you see an error such as `vim.fault.PlatformConfigFault` , which is a catch-all fault indicating that some error has occurred regarding the configuration of the ESXi host. In the vSphere Client, you see a message such as `An error occurred during host configuration.`

This issue is resolved in this release. The fix is to return a `TaskInProgress` warning instead of `PlatformConfigFault` , so that you are aware of the actual issue and retry the installation.

PR 3164439: Certain applications might take too many ESXi file handles and cause performance aggravation

In very rare cases, applications such as NVIDIA virtual GPU (vGPU) might consume so many file handles that ESXi fails to process other services or VMs. As a result, you might see GPU on some nodes to disappear, or report zero GPU memory, or performance degradation.

This issue is resolved in this release. The fix reduces the number of file handles a vGPU VM can consume.

PR 3162963: If parallel volume expand and volume refresh operations on the same VMFS volume run on two ESXi hosts in the same cluster, the VMFS volume might go offline

While a VMFS volume expand operation is in progress on an ESXi host in a vCenter cluster, if on another host a user or vCenter initiates a refresh of the same VMFS volume capacity, such a volume might go offline. The issue occurs due to a possible mismatch in the device size, which is stamped on the disk in the volume metadata during a device rescan, and the device size value in the Pluggable Storage Architecture (PSA) layer on the host, which might not be updated if the device rescan is not complete.

This issue is resolved in this release. The fix improves the resiliency of the volume manager code to force a consecutive refresh of the device attributes and comparison of the device sizes again if vCenter reports a mismatch in the device size.

PR 3161690: CPU usage of ESXi hosts might intermittently increase in environments that use a Vigor router

Due to a rare race condition, when a VM power off command conflicts with a callback function by a Vigor router, you might see increased CPU usage on ESXi hosts, for example, after an upgrade.

This issue is resolved in this release.

PR 3165374: ESXi hosts might become unresponsive and fail with a purple diagnostic screen during TCP TIME_WAIT

The TCP slow timer might starve TCP input processing while it covers the list of connections in `TIME_WAIT` closing expired connections due to contention on the global TCP pcbinfo lock. As a result, the VMkernel might fail with a purple diagnostic screen and the error `Spin count exceeded - possible deadlock` while cleaning up `TCP TIME_WAIT` sockets. The backtrace points to tcpip functions such as `tcp_slowtimo()` or `tcp_twstart()` .

This issue is resolved in this release. The fix adds a new global lock to protect the list of connections in `TIME_WAIT` and to acquire the TCP pcbinfo lock only when closing an expired connection.

PR 3166818: If any of the mount points that use the same NFS server IP returns an error, VAAI-NAS might mark all mount points as not supported

When you use a VAAI-NAS vendor plug-in, multiple file systems on an ESXi host use the same NFS server IP to create a datastore. For certain NAS providers, if one of the mounts returns a `VIX_E_OBJECT_NOT_FOUND (25)` error during the `startSession` call, hardware acceleration for all file systems with the same NFS server IP might become unsupported. This issue occurs when an ESXi host mounts a directory on an NFS server, but that directory is not available at the time of the `startSession` call, because, for example, it has been moved from that NFS server.

This issue is resolved in this release. The fix makes sure that VAAI-NAS marks as not supported only mounts that report an error.

PR 3112692: The smartpqi driver cannot get the location of ThinkSystem PM1645a SAS SSD devices

In rare cases, the `smartpqi plugin in LSU service` might get a longer serial number string from the VPD page 0x80 than the actual serial number, and the device lookup in the cache fails. As a result, when you run the command `esxcli storage core device physical get -d <device_id>` to get a device location, you see an error such as `Unable to get location for device. Device is not found.` .

This issue is resolved in this release. The fix makes sure that the `smartpqi plugin in LSU service` always checks the correct serial number length and finds the device location.

PR 3100030: An ESXi host fails with a purple diagnostic screen indicating VMFS heap corruption

A race condition in the host cache of a VMFS datastore might cause heap corruption and the ESXi host fails with a purple diagnostic screen and a message such as:

```
PF Exception 14 in world xxxxx:res3HelperQu IP 0xxxxxxe2 addr 0xXXXXXXXXX
```

This issue is resolved in this release.

PR 3121216: If the Internet Control Message Protocol (ICMPA) is not active, ESXi host reboot might take long after an upgrade

If ICMPA is not active on the NFS servers in your environment, after upgrading your system, ESXi hosts reboot might take an hour to complete, because restore operations for NFS datastores fail. NFS uses the `vmkping` utility to identify reachable IPs of the NFS servers before executing a mount operation and when ICMP is not active, mount operations fail.

This issue is resolved in this release. To remove dependency on the ICMP protocol to find reachable IPs, the fix adds socket APIs to ensure that IPs on a given NFS server are available.

PR 3098760: ESXi hosts randomly disconnect from the Active Directory domain or vCenter due to Likewise memory exhaustion

Memory leaks in Active Directory operations and related libraries, or when smart card authentication is enabled on an ESXi host, might lead to Likewise memory exhaustion.

This issue is partially resolved in this release. For more information, see VMware knowledge base article 78968.

PR 3118402: The NTP monitoring function returns intermittent time sync failure in the time services test report even when the ESXi host system clock is actually in sync

The time services monitoring infrastructure periodically queries the NTP daemon, ntpd, for time sync status on ESXi hosts. Intermittent query failures might occur due to timeouts in the socket call to read such status information. As a result, you might see time sync failure alerts in the NTP test reports.

This issue is resolved in this release. The fix makes sure that NTP monitoring queries do not fail.

PR 3159168: You see multiple "End path evaluation for device" messages in the vmkernel.log

A periodic device probe that evaluates the state of all the paths to a device might create multiple unnecessary `End path evaluation for device` messages in the `vmkernel.log` file on a release build.

This issue is resolved in this release. The fix restricts `End path evaluation for device` messages to only non-release builds, such as beta. You must enable the VERBOSE log level to see such logs.

PR 3101512: You see a warning for lost uplink redundancy even when the uplink is active

If you quickly remove the network cable from a physical NIC and reinsert it, the ESXi host agent, hostd, triggers an event to restore uplink redundancy, but in some cases, although the uplink restores in a second, you still see a misleading alarm for lost uplink redundancy.

This issue is resolved in this release.

PR 3161473: Operations with stateless ESXi hosts might not pick the expected remote disk for system cache, which causes remediation or compliance issues

Operations with stateless ESXi hosts, such as storage migration, might not pick the expected remote disk for system cache. For example, you want to keep the new boot LUN as LUN 0, but vSphere Auto Deploy picks LUN 1.

This issue is resolved in this release. The fix provides a consistent way to sort the remote disks and always pick the disk with the lowest LUN ID. To make sure you enable the fix, follow these steps:

1. On the Edit host profile page of the Auto Deploy wizard, select **Advanced Configuration Settings** > **SystemImage Cache Configuration** > **System Image Cache Configuration**
2. In the **System Image Cache Profile Settings** drop-down menu, select **Enable stateless caching on the host**.
3. Edit **Arguments** for first disk by replacing **remote** with **sortedremote** and/or **remoteesx** with **sortedremoteesx**.

ESXi-7.0U3o-22348816-no-tools

Profile Name	ESXi-7.0U3o-22348816-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	VMware, Inc.
Release Date	September 28, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.105.22348816 • VMware_bootbank_native-misc-drivers_7.0.3-0.105.22348816 • VMware_bootbank_vsanhealth_7.0.3-0.105.22348816 • VMware_bootbank_crx_7.0.3-0.105.22348816 • VMware_bootbank_esx-xserver_7.0.3-0.105.22348816 • VMware_bootbank_vdfs_7.0.3-0.105.22348816 • VMware_bootbank_cpu-microcode_7.0.3-0.105.22348816 • VMware_bootbank_esx-base_7.0.3-0.105.22348816

	• VMware_bootbank_vsan_7.0.3-0.105.22348816 • VMware_bootbank_esxio-combiner_7.0.3-0.105.22348816 • VMware_bootbank_esx-ui_2.11.2-21988676 • VMware_bootbank_bmcal_7.0.3-0.105.22348816 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.105.22348816 • Mware_bootbank_trx_7.0.3-0.105.22348816 • VMware_bootbank_loadesx_7.0.3-0.105.22348816 • VMware_bootbank_esx-update_7.0.3-0.105.22348816 • VMW_bootbank_lsi-msgpt3_17.00.12.00-2vmw.703.0.105.22348816 • VMware_bootbank_lsuv2-smartpqiv2-plugin_1.0.0-9vmw.703.0.105.22348816 • VMW_bootbank_nvme-pcie_1.2.3.16-3vmw.703.0.105.22348816 • VMW_bootbank_vmw-ahci_2.0.11-2vmw.703.0.105.22348816 • VMW_bootbank_iavmd_2.7.0.1157-3vmw.703.0.105.22348816
PRs Fixed	3244098, 3216958, 3245763, 3242021, 3246132, 3253205, 3256804, 3239170, 3251981, 3215370, 3117615, 3248478, 3252676, 3235496, 3238026, 3236064, 3224739, 3224306, 3223755, 3216958, 3233958, 3185125, 3219264, 3221620, 3218835, 3185560, 3221099, 3211625, 3221860, 3228586, 3224604, 3223539, 3222601, 3217258, 3213041, 3216522, 3221591, 3216389, 3220004, 3217633, 3216548, 3216449, 3156666, 3181574, 3180746, 3155476, 3211807, 3154090, 3184008, 3183519, 3183519, 3209853, 3100552, 3187846, 3113263, 3176350, 3185827, 3095511, 3184425, 3186351, 3186367, 3154090, 3158524, 3181601, 3180391, 3180283, 3184608, 3181774, 3155476, 3163361, 3182978, 3184368, 3160456, 3164575, 3181901, 3184871, 3166818, 3157195, 3164355, 3163271, 3112194, 3161690, 3261925, 3178589, 3178721, 3162963, 3168950, 3159168, 3158491, 3158866, 3096769, 3165374, 3122037, 3098760, 3164439, 3161473, 3162790, 3100030, 3096974, 3161473, 3165651, 3083007, 3118240, 3151076, 3118402, 3160480, 3156627, 3158531, 3162499, 3158512, 3053430, 3153395, 3117615, 3099192, 3158508, 3115870, 3119834, 3158220, 3110401, 2625439, 3099357, 3152811, 3108979, 3120165, 3245953, 3178109, 3211395, 3164477, 3119959, 3164462, 3036883, 3112692, 3218578, 3224847
Related CVE numbers	N/A

This patch updates the following issues:

PR 3187846: Setting the screen resolution of a powered off, encrypted virtual machine does not always work when manually editing the VMX file

If you manually specify the screen resolution of a powered off, encrypted virtual machine by editing the VMX file, the change might not take effect.

This issue is resolved in this release.

PR 3253205: Static IPv6 gateway disappears in 18 hours

If you configure a static IPv6 gateway address in your vSphere environment, such gateways might no longer exist in up to 18 hours due to a timeout.

This issue is resolved in this release. The fix removes the existing timeout for static gateways.

PR 3272532: You see speed as Half Duplex after changing the speed from Auto to Full on a VMNIC

In some cases, length checks during the parsing of duplex TLVs in an environment with active Cisco Discovery Protocol (CDP) might fail. As a result, when you change the speed from **Auto** to **Full** on a physical NIC on peer devices you do not see the real duplex value in the TLV under the neighbor information, but the default Half Duplex value.

This issue is resolved in this release.

PR 3251981: An NFSv4.1 file might appear to be empty even though it contains data

When you open an existing NFSv4.1 file with write only access, if for some reason the NFS client opens again the same file with read only access, read operations from the client might return no data although the file is not empty.

This issue is resolved in this release.

PR 3116601: When you override the default gateway for the vSAN VMkernel adapter on an ESXi host, the vSphere HA agent on the host displays as inaccessible

In some cases, when you override the default gateway for the vSAN VMkernel adapter on an ESXi host, the Fault Domain Manager (FDM), which is the agent that vSphere HA deploys on ESX hosts, might stop receiving Internet Control Message Protocol (ICMP) pings. As a result, FDM might issue false cluster alarms that the vSphere HA agent on the host cannot reach some management network addresses of other hosts.

This issue is resolved in this release.

PR 3251801: vSphere vMotion operation from a 6.7.x ESXi host with an Intel Ice Lake CPU fails with msg.checkpoint.cpucheck.fail

vSphere vMotion operations by using either the vSphere Client or VMware Hybrid Cloud Extension (HCX) from an Intel Ice Lake CPU host running ESXi 6.7.x fails with an error such as `msg.checkpoint.cpucheck.fail`. In the vSphere Client, you see a message that cpuid.PSFD is not supported on the target host. In HCX, you see a report such as `A general system error occurred: vMotion failed:`.

This issue is resolved in this release.

PR 3036883: A SAS path might be lost during upgrade of lsi_msgpt3 drivers

Upgrading `lsi_msgpt3` drivers of version `17.00.12.00-1` and earlier might cause storage connections and VMs on ESXi host to become unresponsive due to a lost SAS path. In the VMkernel logs, you see error messages such as:

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: NMP: nmpDeviceAttemptFailover:640:
Retry world failover device "naa.6000d310045e2c000000000000000043" - issuing command
0x459acc1f5dc0
```

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: vmw_psp_rr: psp_rrSelectPath:2177: Could
not select path for device "naa.6000d310045e2c000000000000000043".
```

```
2022-06-19T05:25:51.949Z cpu26:2097947)WARNING: NMP: nmpDeviceAttemptFailover:715: Retry
world failover device "naa.6000d310045e2c000000000000000043" - failed to issue command due
to Not found (APD), try again...
```

This issue is resolved in this release. If you already face the issue, rescan your storage after failing back on storage controller to recover the paths and storage connections.

PR 3224739: You see alarms for dropped syslog messages

If the network throughput of your vSphere system does not align with the speed at which log messages are generated, some of the log messages sent to the remote syslog server might drop. As a result, in the vSphere Client you see host errors of type `Triggered Alarm` and in the logs, you see warnings such as `ALERT: vmsyslog logger xxxx:514 lost yyyy log messages`.

This issue is resolved in this release. The fix improves the network logging performance of the logging service to reduce the number of such lost log messages.

PR 3247027: If any failure occurs during a vSphere vMotion migration of NVIDIA virtual GPU (vGPU) VM, the destination ESXi host might fail with a purple diagnostic screen

In very rare cases, if any type of failure occurs during a vSphere vMotion migration of a vGPU VM, the vMotion operation is marked as a failure while a specific internal operation is in progress. As a result, the destination ESXi host might fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3095511: The SFCB service intermittently fails and generates "sfcb-vmware_bas-zdump" files on multiple ESXi hosts

In very rare cases, when the SFCB service tries to access an uninitialized variable, the service might fail with dump file such as `sfcb-vmware_bas-zdump.000` . The issue occurs because accessing an uninitialized variable can cause the SFCB process to keep requesting memory until it exceeds the heap allocation.

This issue is resolved in this release.

PR 3218578: You see wrong device descriptions of some Lenovo ThinkSystem boot RAID adapters

In a vSphere client interface, such as the vSphere Client, or when you run commands such as `lspci` and `esxcfg-scsidevs -a` from the ESXi shell, you might see the device names of some Lenovo-branded boot SATA/NVMe adapters as the generical names of the controller chips they use. For example, **Lenovo ThinkSystem M.2 with Mirroring Enablement Kit** is displayed as **88SE9230 PCIe SATA 6GB/s controller**.

This issue is resolved in this release.

PR 3256804: File server loses connectivity after failover when running vSAN File Service on NSX overlay network

If vSAN File Service is running on an NSX overlay network, the file server might lose connectivity after it fails over from one agent VM to another agent VM. The file server can failover when reconfiguring file service domain from such without Active Directory(AD) to such with AD, or if vSAN detects unhealthy behavior in the file server, file share, or AD server. If file server connectivity is lost after a failover, File Service clients cannot access the file share. The following health warning might be reported:

```
One or more DNS servers is not reachable.
```

This issue is resolved in this release.

PR 3217633: vSAN management service on the orchestration host malfunctions during vCenter restart

This issue can occur on vSAN clusters where vCenter is deployed. If multiple cluster shutdown operations are performed, the `/etc/vmware/vsan/vsanperf.conf` file on the orchestration host can contain two versions of the following management VM: `vc_vm_moIdvc_vm_moid` . These configuration options conflict with each other and can cause the vSAN management service to malfunction.

This issue is resolved in this release.

PR 3224306: When you change the ESXi syslog setting syslog.global.logDir, if syslog.global.logDirUnique is active, you might see 2 levels of <hostname> subdir under the logdir path

After upgrading an ESXi host to 7.0 Update 3c and later, if you change the syslog setting `syslog.global.logDir` and the `syslog.global.logDirUnique` setting is active, you might see 2 levels of `<hostname>` subdirs under the `logdir` path on the host. The `syslog.global.logDirUnique` setting is useful if the same NFS directory is configured as the `Syslog.global.LogDir` by multiple ESXi hosts, as it creates a subdirectory with the name of the ESXi host under `logdir` .

This issue is resolved in this release.

PR 3223755: ESXi syslog daemon fails to resume transmitting logs to the configured SSL remote syslog server once a drop in the network connectivity restores

If a remote SSL syslog server temporarily loses connectivity, the ESXi syslog daemon might fail to resume transmitting logs after connectivity restores and you must restart the service to re-activate transmissions. The issue occurs due to some unhandled exceptions while the ESXi syslog daemon tries to restore connection to the SSL remote syslog server.

This issue is resolved in this release. The fix adds a generic catch for all unhandled exceptions.

PR 3185536: vSAN cluster remediation error after vCenter upgrade to 7.0 Update 3

When you upgrade vCenter from version 6.5.x to 7.0 Update 3, and reconfigure the vSAN cluster, a vSAN cluster remediation is triggered, but in some cases fails.

This issue is resolved in this release.

PR 3110401: The Explicit Congestion Notification (ECN) setting is not persistent on ESXi host reboot

ECN, specified in RFC 3168, allows a TCP sender to reduce the transmission rate to avoid packet drops and is activated by default. However, if you change the default setting, or manually deactivate ECN, such changes to the ESXi configuration might not persist after a reboot of the host.

This issue is resolved in this release.

PR 3153395: Upon refresh, some dynamic firewalls rules might not persist and lead to vSAN iSCSI Target service failure

If you frequently run the command `esxcli network firewall refresh` , a race condition might cause some dynamic firewalls rules to be removed upon refresh or load. As a result, some services such as the vSAN iSCSI Target daemon, which provides vSAN storage with iSCSI protocol, might fail.

This issue is resolved in this release.

PR 3096769: You see high latency for VM I/O operations in a vSAN cluster with Unmap activated

This issue affects vSAN clusters with Unmap activated. A problem in Unmap handling in LSOM creates log congestion. The log congestion can cause high VM I/O latency.

This issue is resolved in this release.

PR 3163361: The Audit Record Storage Capacity parameter does not persist across ESXi host reboots

After an ESXi host reboot, you see the **Audit Record Storage Capacity** parameter restored to the default value of 4 MiB, regardless of any previous changes.

This issue is resolved in this release.

PR 3162496: If the Internet Control Message Protocol (ICMPA) is not active, ESXi host reboot might take long after upgrading to vSphere 8.0 and later

If ICMPA is not active on the NFS servers in your environment, after upgrading your system to vSphere 8.0 and later, ESXi hosts reboot might take an hour to complete, because restore operations for NFS datastores fail. NFS uses the `vmkping` utility to identify reachable IPs of the NFS servers before executing a mount operation and when ICMP is not active, mount operations fail.

This issue is resolved in this release. To remove dependency on the ICMP protocol to find reachable IPs, the fix adds socket APIs to ensure that IPs on a given NFS server are available.

PR 3220004: VBS-enabled Windows VMs might fail with a blue diagnostic screen when an ESXi host is under memory pressure

Windows VMs with virtualization-based security (VBS) enabled might intermittently fail with a blue diagnostic screen during memory-heavy operations such as deleting snapshots or consolidating disks. The BSOD has the following signature:

```
DRIVER_VERIFIER_DMA_VIOLATION (e6)
An illegal DMA operation was attempted by a driver being verified.
```

Arguments:

```
Arg1: 0000000000000026, IOMMU detected DMA violation.
Arg2: 0000000000000000, Device Object of faulting device.
Arg3: xxxxxxxxxxxxxxxx, Faulting information (usually faulting physical address).
Arg4: 0000000000000008, Fault type (hardware specific).
```

This issue is resolved in this release.

PR 3162905: ESXi hosts might intermittently disconnect from vCenter in case of memory outage

In rare cases, if vCenter fails to allocate or transfer active bitmaps due to an alert for insufficient memory for any reason, the hostd service might repeatedly fail and you cannot reconnect the host to the vCenter.

This issue is resolved in this release. The fix makes sure that in such cases you see an error rather than the hostd service failure.

PR 3108979: Staging ESXi patches and ESXi upgrade tasks might become indefinitely unresponsive due to a log buffer limit

If a large string or log exceed the python log buffer limit of 16K, the logger becomes unresponsive. As a result, when you stage ESXi patches on a host by using the vSphere Client, the process responsible for completing the staging task on ESXi might become indefinitely unresponsive. The task times out and reports an error. The issue occurs also when you remediate ESXi hosts by using a patch baseline.

This issue is resolved in this release. The fix breaks the large input string into smaller chunks for logging.

PR 3219264: vSAN precheck for maintenance mode or disk decommission doesn't list objects that might lose accessibility

This issue affects objects with resyncing components, and some components reside on a device to be removed or placed into maintenance mode. When you run a precheck with the **No-Action** option, the precheck does not evaluate the object correctly to report it in the `inaccessibleObjects` list.

This issue is resolved in this release. Precheck includes all affected objects in the `inaccessibleObjects` list.

PR 3186545: Vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable

Some third-party tools for vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable.

This issue is resolved in this release.

PR 3221591: ESXi NVMe/TCP initiator fails to recover paths after target failure recovery

When a NVMe/TCP target recovers from a failure, ESXi cannot recover the path.

This issue is resolved in this release.

PR 3186351: You see an override flag of NIC teaming, security, or traffic shaping policy on a portgroup unexpectedly enabled post an ESXi host reboot

In some cases, a networking configuration might not persist in the ESXi ConfigStore and you see an override flag of NIC teaming, security, or traffic shaping policy on a portgroup unexpectedly enabled post an ESXi host reboot.

This issue is resolved in this release.

PR 3162790: The sfcb daemon might fail with a core dump while installing a third-party CIM provider

The sfcb daemon might try to access already freed memory when registering a CIM provider and fail with a core dump while installing a third-party CIM provider, such as Dell OpenManage Server Administrator for example.

This issue is resolved in this release.

PR 3157195: ESX hosts might fail with a purple diagnostic screen and an error NMI IPI: Panic requested by another PCPU

The resource pool cache is a VMFS specific volume level cache that stores the resource clusters corresponding to the VMFS volume. While searching for priority clusters, the cache flusher workflow iterates through a large list of cached resource clusters, which can cause lockup of the physical CPUs. As a result, ESX hosts might fail with a purple diagnostic screen. In the `logDump` file, you see an error such as:

```
^[[7m2022-10-22T07:56:47.322Z cpu13:2101160)WARNING: Heartbeat: 827: PCPU 0 didn't have a heartbeat for 7 seconds, timeout is 14, 1 IPIs sent; *may* be locked up.^[[0m^
```

```
[[31;1m2022-10-22T07:56:47.322Z cpu0:2110633)ALERT: NMI: 710: NMI IPI: RIPOFF(base):RBP:CS
```

This issue is resolved in this release.

PR 3230493: If a delta sync runs while the target vSphere Replication server is not active, Windows virtual machines might become unresponsive

If the target Sphere Replication server is not active during a delta sync, the synchronization process cannot complete and Windows virtual machines become unresponsive.

This issue is resolved in this release. The fix makes sure that no delta sync jobs start when a Sphere Replication server is not active.

PR 3122037: ESXi ConfigStore database fills up and writes fail

Stale data related to block devices might not be deleted in time from the ESXi ConfigStore database and cause an out of space condition. As a result, write operations to ConfigStore start to fail. In the backtrace, you see logs such as:

```
2022-12-19T03:51:42.733Z cpu53:26745174)WARNING: VisorFSRam: 203: Cannot extend visorfs file /etc/vmware/configstore/current-store-1-journal because its ramdisk (configstore) is full .
```

This issue is resolved in this release.

PR 3246132: You see a system clock drift on an ESXi host after synchronization with the NTP server fails

If connectivity between the NTP server and an ESXi host is delayed for some reason, the system clock on the ESXi host might experience a drift. When you run the `vsish` command `vsish -e get /system/ntpclock/clockData` , you might see a large negative value for the `adjtime` field. For example:

```
NTP clock data {
...  adjtime() (usec):-309237290312 <<<<<<
...
}
```

This issue is resolved in this release.

PR 3185560: vSphere vMotion operations for virtual machines with swap files on a vSphere Virtual Volumes datastore intermittently fail after a hot extend of the VM disk

vSphere vMotion operations for virtual machines with swap files on a vSphere Virtual Volumes datastore might fail under the following circumstances:

A VM that runs on ESXi host A is migrated to ESXi host B, then the VM disk is hot extended, and the VM is migrated back to ESXi host A. The issue occurs due to stale statistics about the swap virtual volume.

This issue is resolved in this release.

PR 3236207: You cannot unmount an NFS v3 datastore from a vCenter system because the datastore displays as inaccessible

While unmounting an NFSv3 datastore from a vCenter system by using either the vSphere Client or ESXCLI, you might see the datastore either as inaccessible, or get an `Unable to Refresh` error. The issue occurs when a hostd cache refresh happens before NFS deletes the mount details from ConfigStore, which creates a rare race condition.

This issue is resolved in this release.

PR 3236064: Compliance or remediation scans by using vSphere Lifecycle Manager might take long on ESXi hosts with a large number of datastores

Compliance or remediation scans by using vSphere Lifecycle Manager include an upgrade precheck that lists all volumes attached to an ESXi host, their free space, versions, and other details. If a host has many datastores attached, each with a large capacity, the precheck can take long. The time is multiplied by the number of baselines attached to the cluster or host.

This issue is resolved in this release. If you already face the issue, disconnect the attached datastores while performing the remediation or compliance scans and reattach them after the operations complete.

PR 3245763: During a vSphere vMotion operation, destination ESXi hosts with a Distributed Firewall (DFW) enabled might fail with a purple diagnostic screen

If the destination host in a vSphere vMotion operation has a DFW enabled, a rare race condition might cause the host to fail with a purple diagnostic screen.

This issue is resolved in this release.

PR 3158866: Virtual machines might become unresponsive during VMFS volume expansion due to a Logical Volume Manager (LVM) check

If a VMFS volume expansion operation happens during a LVM probe to update volume attributes, such as the size of the VMFS partition backing of the VMFS volume, the current size of the VMFS volume might not match the LVM metadata on the disk. As a result, LVM marks such a volume offline and virtual machines on that volume become unresponsive.

This issue is resolved in this release. The fix improves Input Output Control (IOCTL) to speed up the update of device attributes and avoid such cases.

PR 3152717: vSphere Auto Deploy workflows might fail after an upgrade to vCenter Server 7.0 Update 3j or later

Due to a networking issue in reverse proxy configuration environments, vSphere Auto Deploy workflows might fail after an upgrade to vCenter Server 7.0 Update 3j or later. In the ESXi management console and in the `/var/log/vmware/rbd/rbd-cgi.log file` you see an HTTP client error.

This issue is resolved in this release. The fix makes sure Auto Deploy workflows run successfully in reverse proxy configuration environments.

PR 3185125: Virtual SLIT table not populated for the guest OS when using sched.nodeX.affinity

When you specify virtual NUMA node affinity, the vSLIT table might not be populated and you see the following error in `vmware.log`: `vSLIT: NumaGetLatencyInfo failed with status: 195887107.`

This happens when setting node affinity as follows:

```
numa.slit.enable = "TRUE"

sched.node0.affinity = 0

sched.node1.affinity = 1

...sched.nodeN.affinity = N
```

This issue is resolved in this release. If you already face the issue, specify VCPU affinity to physical CPUs on the associated NUMA nodes, instead of node affinity.

For example:

```
numa.slit.enable = "TRUE"

sched.vcpu0.affinity = "0-7"

sched.vcpu1.affinity = "0-7"

...sched.vcpuN.affinity = "Y-Z"
```

PR 3181774: You do not see an error when you attach a CBT enabled FCD to a VM with CBT disabled

Attaching a First Class Disk (FCD) with Changed Block Tracking (CBT) to a VM with CBT disabled does not throw a detailed error, but the operation cannot take effect. In the backtrace, you might see an error message such as `InvalidState` , which is generic and does not provide details on the issue.

This issue is resolved in this release. The fix adds the error message `Cannot attach a CBT enabled fcd: {path} to CBT disabled VM.` to the logs of the hostd service and adds a status message for the task in the vSphere Client.

PR 3185827: You see trap files in a SNMP directory under /var/spool even though SNMP is not enabled

After the hostd service starts, for example after an ESXi host reboot, it might create a SNMP directory under `/var/spool` and you see many `.trp` files to pile in this directory.

This issue is resolved in this release. The fix makes sure that the directory `/var/spool/snmp` exists only when SNMP is enabled.

PR 3082867: An ESXi host might fail with a purple diagnostic screen after a replicated virtual machine migrates to the host

In some environments, when a replicated virtual machine migrates to a certain ESXi host, during a full sync, some `SCSI WRITE` commands might target address ranges past the end of the transfer map. As a result, the ESXi host might fail with a purple diagnostic screen and a backtrace such as:

```
#0 DLM_free (msp=0x43238f2c9cc0, mem=mem@entry=0x43238f6db860, allowTrim=allowTrim@entry=1
'\001') at bora/vmkernel/main/dlmalloc.c:4924

#1 0x000041802a151e01 in Heap_Free (heap=0x43238f2c9000, mem=<optimized out>) at bora/
vmkernel/main/heap.c:4217

#2 0x000041802a3b0fa1 in BitVector_Free (heap=<optimized out>, bv=<optimized out>) at
bora/vmkernel/util/bitvector.c:94

#3 0x000041802b9f4f3f in HbrBitmapFree (bitmap=<optimized out>) at bora/modules/vmkernel/
hbr_filter/hbr_bitmap.c:91
```

This issue is resolved in this release.

PR 3162499: During service insertion for NSX-managed workload VMs, some VMS might become intermittently unresponsive, and the virtual device might reset

During service insertion for NSX-managed workload VMs, a packet list might be reinjected from the input chain of one switchport to another switchport. In such cases, the source switchport does not correspond to the actual `portID` of the input chain and the virtual device does not get completion status for the transmitted frame. As a result, when you run a service insertion task, some VMs might become intermittently unresponsive due to network connectivity issues.

This issue is resolved in this release.

PR 3219441: You cannot send keys to a guest OS by using the browser console in the ESXi Host Client

In the ESXi Host Client, when you open the browser console of a virtual machine and select **Guest OS > Send keys**, when you select a key input, for example **Ctrl-Alt-Delete**, the selection is not sent to the guest OS.

This issue is resolved in this release.

PR 3209853: Windows VMs might fail with a blue diagnostic screen with 0x5c signature due to platform delays

Windows VMs might fail with a blue diagnostic screen with the following signature due to a combination of factors involving the Windows timer code and platform delays, such as storage or network delays:

`HAL_INITIALIZATION_FAILED (0x5c)` (This indicates that the HAL initialization failed.)

Arguments:

```
Arg1: 0000000000000115, HAL_TIMER_INITIALIZATION_FAILURE
Arg2: fffff7ea800153e0, Timer address
Arg3: 00000000000014da, Delta in QPC units (delta to program the timer with)
Arg4: ffffffffc0000001, invalid status code (STATUS_UNSUCCESSFUL)
```

Checks done by HPET timers in Windows might fail due to such platform delays and cause the issue.

This issue is resolved in this release.

PR 3178109: vSphere Lifecycle Manager compliance check fails with "An unknown error occurred while performing the operation"

The base ESXi image contains driver components that can be overridden by higher version async driver components packaged by an OEM add-on. If such a component is manually removed on a host, the compliance check of the vSphere Lifecycle Manager might fail unexpectedly. In the vSphere Client, you see errors such as `Host status is unknown` and `An unknown error occurred while performing the operation.`

This issue is resolved in this release.

PR 3180634: Performance of certain nested virtual machines on AMD CPUs might degrade

Nested virtual machines on AMD CPUs with operational systems such as Windows with virtualization-based security (VBS) might experience performance degradation, timeouts, or unresponsiveness due to an issue with the virtualization of AMD's Rapid Virtualization Indexing (RVI), also known as Nested Page Tables (NPT).

This issue is resolved in this release.

PR 3223539: Some vmnics might not be visible after an ESXi host reboot due to a faulty NVMe device

If an NVMe device fails during the attach phase, the NVMe driver disables the NVMe controller and resets the hardware queue resources. When you try to re-attach the device, a mismatch between the hardware and driver queue pointers might cause an IOMMU fault on the NVMe device, which leads to memory corruption and failure of the vmkdevmgr service. As a result, you do not see some vmnics in your network.

This issue is resolved in this release.

PR 3218835: When you disable or suspend vSphere Fault Tolerance, virtual machines might become unresponsive for about 10 seconds

When you disable or suspend vSphere FT, some virtual machines might take about 10 seconds to release vSphere FT resources. As a result, such VMs become temporarily unresponsive to network requests or console operations.

This issue is resolved in this release.

PR 3181901: ESXi host becomes unresponsive and you cannot put the host in Maintenance Mode or migrate VMs from that host

Asynchronous reads of metadata on a VMFS volume attached to an ESXi host might cause a race condition with other threads on the host and make the host unresponsive. As a result, you cannot put the host in Maintenance Mode or migrate VMs from that host.

This issue is resolved in this release.

PR 3156666: Packets with length less than 60 bytes might drop

An ESXi host might add invalid bytes, other than zero, to packets with less than 60 bytes. As a result, packets with such invalid bytes drop.

This issue is resolved in this release.

PR 3180283: When you migrate a VM with recently hot-added memory, an ESXi host might repeatedly fail with a purple diagnostic screen

Due to a race condition while the memory hotplug module recomputes the NUMA memory layout of a VM on a destination host after migration, an ESXi host might repeatedly fail with a purple diagnostic screen. In the backtrace, you see errors such as:

```
0x452900262cf0:[0x4200138fee8b]PanicvPanicInt@vmkernel#nover+0x327 stack: 0x452900262dc8,
0x4302f6c06508, 0x4200138fee8b, 0x420013df1300, 0x452900262cf0  0x452900262dc0:
[0x4200138ff43d]Panic_WithBacktrace@vmkernel#nover+0x56 stack: 0x452900262e30,
0x452900262de0, 0x452900262e40, 0x452900262df0, 0x3e7514  0x452900262e30:
[0x4200138fbb90]NMI_Interrupt@vmkernel#nover+0x561 stack: 0x0, 0xf48, 0x0,
0x0, 0x0  0x452900262f00:[0x420013953392]IDTNMIWork@vmkernel#nover+0x7f stack:
0x420049800000, 0x4200139546dd, 0x0, 0x452900262fd0, 0x0  0x452900262f20:
[0x4200139546dc]Int2_NMI@vmkernel#nover+0x19 stack: 0x0, 0x42001394e068,
0xf50, 0xf50, 0x0  0x452900262f40:[0x42001394e067]gate_entry@vmkernel#nover
+0x68 stack: 0x0, 0x43207bc02088, 0xd, 0x0, 0x43207bc02088  0x45397b61bd30:
[0x420013be7514]NUMASched_PageNum2PhysicalDomain@vmkernel#nover+0x58 stack:
0x1, 0x420013be34c3, 0x45396f79f000, 0x1, 0x100005cf757  0x45397b61bd50:
[0x420013be34c2]NUMASched_UpdateAllocStats@vmkernel#nover+0x4b stack: 0x100005cf757, 0x0,
0x0, 0x4200139b36d9, 0x0  0x45397b61bd80:[0x4200139b36d8]VmMem_NodeStatsSub@vmkernel#nover
+0x59 stack: 0x39, 0x45396f79f000, 0xbce0dbf, 0x100005cf757, 0x0  0x45397b61bdc0:
[0x4200139b4372]VmMem_FreePageNoBackmap@vmkernel#nover+0x8b stack: 0x465ec0001be0, 0xa,
0x465ec18748b0, 0x420014e7685f, 0x465ec14437d0
```

This issue is resolved in this release.

PR 3100552: ESXi booting times out after five minutes and the host automatically reboots

During initial ESXi booting, when you see the **Loading VMware ESXi** progress bar, if the bootloader takes more than a total of five minutes to load all the boot modules before moving on to the next phase of booting, the host firmware times out the boot process and resets the system.

This issue is resolved in this release. With ESXi 7.0 Update 3o, the ESXi bootloader resets the five-minute timeout after each boot module loads.

PR 3184368: The durable name of a SCSI LUN might not be set

The durable name property for a SCSI-3 compliant device comes from pages `80h` and `83h` of the Vital Product Data (VPD) as defined by the T10 and SMI standards. To populate the durable name, ESXi first sends an inquiry command to get a list of VPD pages supported by the device. Then ESXi issues commands to get data for all supported VPD pages. Due to an issue with the target array, the device might fail a command to get VPD page data for a page in the list with a `not supported` error. As a result, ESXi cannot populate the durable name property for the device.

This issue is resolved in this release. The fix ignores the error on command to get VPD page data, except pages `80h` and `83h` , if that data is not required for the generation of durable name.

PR 3184425: Port scan of a VXLAN Tunnel End Point (VTEP) on an ESXi host might result in an intermittent connectivity loss

Port scan of a VTEP on an ESXi host might result in an intermittent connectivity loss, but only under the following conditions:

1. Your environment has many VTEPs
2. All VTEPs are in the same IP subnet
3. The upstream switch is Cisco ACI

This issue is resolved in this release.

PR 3156627: Changing the mode of the virtual disk on a running virtual machine might cause the VM to fail

If you use the VMware Host Client to edit the disk mode of a running virtual machine, for example from Independent - Nonpersistent to Dependent or Independent - Persistent, the operation fails and might cause the VM to fail. In the `vmware.log` , you see errors such as:

```
msg.disk.notConfigured2] Failed to configure disk 'scsi0:4'. The virtual machine cannot be powered on with an unconfigured disk.
```

```
[msg.checkpoint.continuesync.error] An operation required the virtual machine to quiesce and the virtual machine was unable to continue running.
```

This issue is resolved in this release. The fix blocks changing the mode of an Independent - Nonpersistent disk on a running virtual machine by using the VMware Host Client. The vSphere Client already blocks such operations.

PR 3164477: In VMware Skyline Health Diagnostics, you see multiple warnings for vSAN memory pools

The free heap memory estimation logic for some vSAN memory pools might consider more memory heap than actual and trigger warnings for insufficient memory. As a result, you see `Memory pools (heap)` health warnings for many hosts under the **Physical disks** section in Skyline Health.

This issue is resolved in this release.

PR 3168950: ESXi hosts fail with a purple diagnostic screen while installing VMware NSX-T Data Center due to insufficient TCP/IP heap space

VMware NSX-T Data Center has multiple net stacks and the default TCP/IP heap space might not be sufficient for installation. As a result, ESXi hosts might fail with a purple diagnostic screen.

This issue is resolved in this release. The fix increases the default `TcpipHeapSize` setting to 8 MB from 0 MB and the maximum size to 128 MB from 32 MB. In the vSphere Client, you can change the `TcpipHeapSize` value by navigating to **Hosts and Clusters > Configure > System > Advanced System Settings > TcpipHeadSize**. In vCenter systems with VMware NSX-T Data Center, set the value to 128 MB.

PR 3096974: Rare race condition in I/O filters might cause an ESXi host to fail with a purple diagnostics screen

ESXi hosts in which virtual machines use I/O filters might randomly fail with a purple diagnostics screen and an error such as `#DF Exception 8 IP 0x42002c54b19f SP 0x453a9e8c2000` due to a rare race condition.

This issue is resolved in this release.

PR 3112194: Spherelet might fail to start on an ESXi host due to the execInstalledOnly setting

The `execInstalledOnly` setting is a run time parameter which limits execution of binaries such as applications and vmkernel modules to improve security and guard against breaches and compromises. Some `execInstalledOnly` security checks might interfere with Spherelet, the ESXi UserWorld agent that acts as an extension to the Kubernetes Control Plane, and prevent it to start, even when all files are installed.

This issue is resolved in this release.

PR 3115870: VMware VIB installation might fail during concurrent vendor package installations

When you install update packages from several vendors, such as JetStream Software, Microsoft, and VMware, multiple clients call the same PatchManager APIs and might lead to a race condition. As a result, VMware installation packages

(VIBs) might fail to install. In the logs, you see an error such as `vim.fault.PlatformConfigFault`, which is a catch-all fault indicating that some error has occurred regarding the configuration of the ESXi host. In the vSphere Client, you see a message such as `An error occurred during host configuration.`

This issue is resolved in this release. The fix is to return a `TaskInProgress` warning instead of `PlatformConfigFault`, so that you are aware of the actual issue and retry the installation.

PR 3164439: Certain applications might take too many ESXi file handles and cause performance aggravation

In very rare cases, applications such as NVIDIA virtual GPU (vGPU) might consume so many file handles that ESXi fails to process other services or VMs. As a result, you might see GPU on some nodes to disappear, or report zero GPU memory, or performance degradation.

This issue is resolved in this release. The fix reduces the number of file handles a vGPU VM can consume.

PR 3162963: If parallel volume expand and volume refresh operations on the same VMFS volume run on two ESXi hosts in the same cluster, the VMFS volume might go offline

While a VMFS volume expand operation is in progress on an ESXi host in a vCenter cluster, if on another host a user or vCenter initiates a refresh of the same VMFS volume capacity, such a volume might go offline. The issue occurs due to a possible mismatch in the device size, which is stamped on the disk in the volume metadata during a device rescan, and the device size value in the Pluggable Storage Architecture (PSA) layer on the host, which might not be updated if the device rescan is not complete.

This issue is resolved in this release. The fix improves the resiliency of the volume manager code to force a consecutive refresh of the device attributes and comparison of the device sizes again if vCenter reports a mismatch in the device size.

PR 3161690: CPU usage of ESXi hosts might intermittently increase in environments that use a Vigor router

Due to a rare race condition, when a VM power off command conflicts with a callback function by a Vigor router, you might see increased CPU usage on ESXi hosts, for example, after an upgrade.

This issue is resolved in this release.

PR 3165374: ESXi hosts might become unresponsive and fail with a purple diagnostic screen during TCP TIME_WAIT

The TCP slow timer might starve TCP input processing while it covers the list of connections in `TIME_WAIT` closing expired connections due to contention on the global TCP pcbinfo lock. As a result, the VMkernel might fail with a purple diagnostic screen and the error `Spin count exceeded - possible deadlock` while cleaning up `TCP TIME_WAIT` sockets. The backtrace points to tcpip functions such as `tcp_slowtimo()` or `tcp_twstart()`.

This issue is resolved in this release. The fix adds a new global lock to protect the list of connections in `TIME_WAIT` and to acquire the TCP pcbinfo lock only when closing an expired connection.

PR 3166818: If any of the mount points that use the same NFS server IP returns an error, VAAI-NAS might mark all mount points as not supported

When you use a VAAI-NAS vendor plug-in, multiple file systems on an ESXi host use the same NFS server IP to create a datastore. For certain NAS providers, if one of the mounts returns a `VIX_E_OBJECT_NOT_FOUND (25)` error during the `startSession` call, hardware acceleration for all file systems with the same NFS server IP might become unsupported. This issue occurs when an ESXi host mounts a directory on an NFS server, but that directory is not available at the time of the `startSession` call, because, for example, it has been moved from that NFS server.

This issue is resolved in this release. The fix makes sure that VAAI-NAS marks as not supported only mounts that report an error.

PR 3112692: The smartpqi driver cannot get the location of ThinkSystem PM1645a SAS SSD devices

In rare cases, the `smartpqi plugin in LSU service` might get a longer serial number string from the VPD page 0x80 than the actual serial number, and the device lookup in the cache fails. As a result, when you run the command

`esxcli storage core device physical get -d <device_id>` to get a device location, you see an error such as `Unable to get location for device. Device is not found.`.

This issue is resolved in this release. The fix makes sure that the `smartpqi plugin in LSU service` always checks the correct serial number length and finds the device location.

PR 3100030: An ESXi host fails with a purple diagnostic screen indicating VMFS heap corruption

A race condition in the host cache of a VMFS datastore might cause heap corruption and the ESXi host fails with a purple diagnostic screen and a message such as:

`PF Exception 14 in world xxxxx:res3HelperQu IP 0xxxxxxe2 addr 0xXXXXXXXXX`

This issue is resolved in this release.

PR 3121216: If the Internet Control Message Protocol (ICMPA) is not active, ESXi host reboot might take long after an upgrade

If ICMPA is not active on the NFS servers in your environment, after upgrading your system, ESXi hosts reboot might take an hour to complete, because restore operations for NFS datastores fail. NFS uses the `vmkping` utility to identify reachable IPs of the NFS servers before executing a mount operation and when ICMP is not active, mount operations fail.

This issue is resolved in this release. To remove dependency on the ICMP protocol to find reachable IPs, the fix adds socket APIs to ensure that IPs on a given NFS server are available.

PR 3098760: ESXi hosts randomly disconnect from the Active Directory domain or vCenter due to Likewise memory exhaustion

Memory leaks in Active Directory operations and related libraries, or when smart card authentication is enabled on an ESXi host, might lead to Likewise memory exhaustion.

This issue is partially resolved in this release. For more information, see VMware knowledge base article 78968.

PR 3118402: The NTP monitoring function returns intermittent time sync failure in the time services test report even when the ESXi host system clock is actually in sync

The time services monitoring infrastructure periodically queries the NTP daemon, ntpd, for time sync status on ESXi hosts. Intermittent query failures might occur due to timeouts in the socket call to read such status information. As a result, you might see time sync failure alerts in the NTP test reports.

This issue is resolved in this release. The fix makes sure that NTP monitoring queries do not fail.

PR 3159168: You see multiple "End path evaluation for device" messages in the vmkernel.log

A periodic device probe that evaluates the state of all the paths to a device might create multiple unnecessary `End path evaluation for device` messages in the `vmkernel.log` file on a release build.

This issue is resolved in this release. The fix restricts `End path evaluation for device` messages to only non-release builds, such as beta. You must enable the VERBOSE log level to see such logs.

PR 3101512: You see a warning for lost uplink redundancy even when the uplink is active

If you quickly remove the network cable from a physical NIC and reinsert it, the ESXi host agent, hostd, triggers an event to restore uplink redundancy, but in some cases, although the uplink restores in a second, you still see a misleading alarm for lost uplink redundancy.

This issue is resolved in this release.

PR 3161473: Operations with stateless ESXi hosts might not pick the expected remote disk for system cache, which causes remediation or compliance issues

Operations with stateless ESXi hosts, such as storage migration, might not pick the expected remote disk for system cache. For example, you want to keep the new boot LUN as LUN 0, but vSphere Auto Deploy picks LUN 1.

This issue is resolved in this release. The fix provides a consistent way to sort the remote disks and always pick the disk with the lowest LUN ID. To make sure you enable the fix, follow these steps:

1. On the Edit host profile page of the Auto Deploy wizard, select **Advanced Configuration Settings** > **SystemImage Cache Configuration** > **System Image Cache Configuration**
2. In the **System Image Cache Profile Settings** drop-down menu, select **Enable stateless caching on the host**.
3. Edit **Arguments** for first disk by replacing **remote** with **sortedremote** and/or **remoteesx** with **sortedremoteesx**.

ESXi-7.0U3so-22348808-standard

Profile Name	ESXi-7.0U3so-22348808-standard
Build	For build information, see Patches Contained in This Release.
Vendor	VMware, Inc.
Release Date	September 28, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vsanhealth_7.0.3-0.100.22348808 • VMware_bootbank_crx_7.0.3-0.100.22348808 • VMware_bootbank_vdfs_7.0.3-0.100.22348808 • VMware_bootbank_esxio-combiner_7.0.3-0.100.22348808 • VMware_bootbank_native-misc-drivers_7.0.3-0.100.22348808 • VMware_bootbank_esx-base_7.0.3-0.100.22348808 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.100.22348808 • VMware_bootbank_cpu-microcode_7.0.3-0.100.22348808 • VMware_bootbank_bmcal_7.0.3-0.100.22348808 • VMware_bootbank_esx-ui_2.11.2-21988676 • VMware_bootbank_gc_7.0.3-0.100.22348808 • VMware_bootbank_trx_7.0.3-0.100.22348808 • VMware_bootbank_vsan_7.0.3-0.100.22348808 • VMware_bootbank_esx-xserver_7.0.3-0.100.22348808 • VMware_bootbank_loadesx_7.0.3-0.100.22348808 • VMware_bootbank_esx-update_7.0.3-0.100.22348808 • VMware_locker_tools-light_12.2.6.22229486-22348808
PRs Fixed	3219441, 3239369, 3236018, 3232099, 3232034, 3222887, 3217141, 3213025, 3187868, 3186342, 3164962, 3089785, 3160789, 3098679, 3089785, 3256457, 3178522, 3178519
Related CVE numbers	N/A

This patch updates the following issues:

ESXi 7.0 Update 3o provides the following security updates:

- The cURL library is updated to version 8.1.2.
- The ESXi userworld libxml2 library is updated to version 2.10.4.
- The SQLite library is updated to version 3.42.0.
- The OpenSSL package is updated to version 1.0.2zh.

The cpu-microcode VIB includes the following AMD microcode:

Code Name	FMS	MCU Rev	MCU Date	Brand Names
Bulldozer	0x600f12 (15/01/2)	0x0600063e	2/7/2018	Opteron 6200/4200/3200 Series
Piledriver	0x600f20 (15/02/0)	0x06000852	2/6/2018	Opteron 6300/4300/3300 Series
Zen-Naples	0x800f12 (17/01/2)	0x0800126e	11/11/2021	EPYC 7001 Series
Zen2-Rome	0x830f10 (17/31/0)	0x0830107a	5/17/2023	EPYC 7002/7Fx2/7Hx2 Series
Zen3-Milan-B1	0xa00f11 (19/01/1)	0x0a0011d1	7/10/2023	EPYC 7003/7003X Series
Zen3-Milan-B2	0xa00f12 (19/01/2)	0x0a001234	7/10/2023	EPYC 7003/7003X Series

The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3o:

- **windows.iso**: VMware Tools 12.2.6 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
- **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
  - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
- VMware Tools 10.0.12:
  - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
  - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
- **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
- **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. For more details, see VMware knowledge base article 88698.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- Updating VMware Tools
- VMware Tools for hosts provisioned with Auto Deploy
- What Every vSphere Admin Must Know About VMware Tools
- Earlier versions of VMware Tools
- VMware Tools 12.2.6 Release Notes

The cpu-microcode VIB includes the following Intel microcode:

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x7	4/23/2018	Intel Core i7-620LE Processor

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x4003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x5003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x7002703	3/21/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0xe000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x38	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0xd0003a5	3/30/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x1000230	1/27/2023	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	0xac	2/27/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	0x2c	2/27/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	0x46	2/27/2023	Intel Xeon W-11000E Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	0x2c0001d1	2/14/2023	Intel Xeon Max 9400 Series
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	0x2b000461	3/13/2023	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0xf4	2/23/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0xfa	2/27/2023	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x59	2/26/2023	Intel Xeon E-2300 Series

ESXi-7.0U3so-22348808-no-tools

Profile Name	ESXi-7.0U3so-22348808-no-tools
Build	For build information, see Patches Contained in This Release.
Vendor	VMware, Inc.
Release Date	September 28, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_vsanhealth_7.0.3-0.100.22348808 • VMware_bootbank_crx_7.0.3-0.100.22348808 • VMware_bootbank_vdfs_7.0.3-0.100.22348808 • VMware_bootbank_esxio-combiner_7.0.3-0.100.22348808 • VMware_bootbank_native-misc-drivers_7.0.3-0.100.22348808 • VMware_bootbank_esx-base_7.0.3-0.100.22348808 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.100.22348808 • VMware_bootbank_cpu-microcode_7.0.3-0.100.22348808 • VMware_bootbank_bmcal_7.0.3-0.100.22348808 • VMware_bootbank_esx-ui_2.11.2-21988676 • VMware_bootbank_gc_7.0.3-0.100.22348808 • VMware_bootbank_trx_7.0.3-0.100.22348808

	• VMware_bootbank_vsan_7.0.3-0.100.22348808 • VMware_bootbank_esx-xserver_7.0.3-0.100.22348808 • VMware_bootbank_loadesx_7.0.3-0.100.22348808 • VMware_bootbank_esx-update_7.0.3-0.100.22348808
PRs Fixed	3219441, 3239369, 3236018, 3232099, 3232034, 3222887, 3217141, 3213025, 3187868, 3186342, 3164962, 3089785, 3160789, 3098679, 3089785, 3256457
Related CVE numbers	N/A

This patch updates the following issues:

ESXi 7.0 Update 3o provides the following security updates:

- The cURL library is updated to version 8.1.2.
- The ESXi userworld libxml2 library is updated to version 2.10.4.
- The SQLite library is updated to version 3.42.0.
- The OpenSSL package is updated to version 1.0.2zh.

The cpu-microcode VIB includes the following AMD microcode:

Code Name	FMS	MCU Rev	MCU Date	Brand Names
Bulldozer	0x600f12 (15/01/2)	0x0600063e	2/7/2018	Opteron 6200/4200/3200 Series
Piledriver	0x600f20 (15/02/0)	0x06000852	2/6/2018	Opteron 6300/4300/3300 Series
Zen-Naples	0x800f12 (17/01/2)	0x0800126e	11/11/2021	EPYC 7001 Series
Zen2-Rome	0x830f10 (17/31/0)	0x0830107a	5/17/2023	EPYC 7002/7Fx2/7Hx2 Series
Zen3-Milan-B1	0xa00f11 (19/01/1)	0x0a0011d1	7/10/2023	EPYC 7003/7003X Series
Zen3-Milan-B2	0xa00f12 (19/01/2)	0x0a001234	7/10/2023	EPYC 7003/7003X Series

The cpu-microcode VIB includes the following Intel microcode:

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x1d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x11	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x7	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x2f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Westmere EP	0x206c2 (06/2c/2)	0x03	0x1f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x71a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0xd	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x3b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x21	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x28	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x42e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x49	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x1a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x22	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x12d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0xb000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x2007006	3/6/2023	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x4003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Cascade Lake	0x50657 (06/55/7)	0xbf	0x5003604	3/17/2023	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/ Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x7002703	3/21/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x1c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0xf00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0xe000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0xf0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x38	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0xd0003a5	3/30/2023	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Silver 4300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x1000230	1/27/2023	Intel Xeon D-2700 Series; Intel Xeon D-1700 Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000023	2/22/2023	Intel Atom P5000 Series
Tiger Lake U	0x806c1 (06/8c/1)	0x80	0xac	2/27/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake U Refresh	0x806c2 (06/8c/2)	0xc2	0x2c	2/27/2023	Intel Core i3/i5/ i7-1100 Series
Tiger Lake H	0x806d1 (06/8d/1)	0xc2	0x46	2/27/2023	Intel Xeon W-11000E Series
Sapphire Rapids SP HBM	0x806f8 (06/8f/8)	0x10	0x2c0001d1	2/14/2023	Intel Xeon Max 9400 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sapphire Rapids SP	0x806f8 (06/8f/8)	0x87	0x2b000461	3/13/2023	Intel Xeon Platinum 8400 Series; Intel Xeon Gold 6400/5400 Series; Intel Xeon Silver 4400 Series; Intel Xeon Bronze 3400 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0xf4	2/23/2023	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0xf4	2/23/2023	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0xfa	2/27/2023	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x59	2/26/2023	Intel Xeon E-2300 Series

ESXi7.0U3o - 22348816

Name	ESXi
Version	ESXi7.0U3o - 22348816
Release Date	September 28, 2023
Category	Bugfix
Affected Components	• ESXi Component - core ESXi • ESXi Install/Upgrade • VMware Native AHCI Driver • SMARTPQI LSU Management Plugin • Non-Volatile memory controller driver • Avago (LSI) Native 12Gbps SAS MPT Driver • Intel NVME Driver with VMD Technology
PRs Fixed	3244098, 3216958, 3245763, 3242021, 3246132, 3253205, 3256804, 3239170, 3251981, 3215370, 3117615, 3248478, 3252676, 3235496, 3238026, 3236064, 3224739, 3224306, 3223755, 3216958, 3233958, 3185125, 3219264, 3221620, 3218835, 3185560, 3221099, 3211625, 3221860, 3228586, 3224604, 3223539, 3222601, 3217258, 3213041, 3216522, 3221591, 3216389, 3220004, 3217633, 3216548, 3216449, 3156666, 3181574, 3180746, 3155476, 3211807, 3154090, 3184008, 3183519, 3183519, 3209853, 3100552, 3187846, 3113263, 3176350, 3185827, 3095511, 3184425, 3186351, 3186367, 3154090, 3158524, 3181601, 3180391, 3180283, 3184608, 3181774, 3155476, 3163361, 3182978, 3184368, 3160456, 3164575, 3181901, 3184871, 3166818, 3157195,

	3164355, 3163271, 3112194, 3161690, 3261925, 3178589, 3178721, 3162963, 3168950, 3159168, 3158491, 3158866, 3096769, 3165374, 3122037, 3098760, 3164439, 3161473, 3162790, 3100030, 3096974, 3161473, 3165651, 3083007, 3118240, 3151076, 3118402, 3160480, 3156627, 3158531, 3162499, 3158512, 3053430, 3153395, 3117615, 3099192, 3158508, 3115870, 3119834, 3158220, 3110401, 2625439, 3099357, 3152811, 3108979, 3120165, 3245953, 3178109, 3211395, 3164477, 3119959, 3164462, 3036883, 3112692, 3218578, 3224847
Related CVE numbers	N/A

This patch resolves the issues listed in ESXi-7.0U3o-22348816-standard.

ESXi7.0U3so - 22348808

Name	ESXi
Version	ESXi7.0U3so - 22348808
Release Date	September 28, 2023
Category	Security
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • ESXi Tools Component
PRs Fixed	3219441, 3239369, 3236018, 3232099, 3232034, 3222887, 3217141, 3213025, 3187868, 3186342, 3164962, 3089785, 3160789, 3098679, 3089785, 3256457, 3178522, 3178519
Related CVE numbers	N/A

This patch resolves the issues listed in ESXi-7.0U3so-22348808-standard.

Known Issues

vSAN Issues

PR 2962316: vSAN File Service does not support NFSv4 delegations

vSAN File Service does not support NFSv4 delegations in this release.

Workaround: None

PR 3235496: Applications on a vSAN cluster become intermittently unresponsive

If the advanced option `preferHT` is enabled on an AMD server in a vSAN cluster, the virtual CPUs of a virtual machine run on the same last level cache. When the virtual CPUs are all very busy and an NVMe thread to handle I/Os happens to run also on the same last level cache, the NVMe thread takes very long to complete, because it competes for CPU resources with the busy VMs. As a result, the I/O latency is very high and might lead to intermittent unresponsiveness of storage and applications on the vSAN cluster. In the backlog, you see errors such as `Lost access to volume <uuid> due to connectivity issues. Recovery attempt is in progress and outcome will be reported shortly.`

Workaround: Use the command `esxcli system settings advanced set -o /Misc/vmknvmeCwYield -I 0` to avoid competition between the NVMe completion queue and busy virtual CPUs.

Miscellaneous Issues

Windows or Citrix virtual machines with NVIDIA virtual GPU (vGPU) might intermittently fail with a blue diagnostics screen

After upgrading to ESXi 7.0 Update 3o, some Windows or Citrix vGPU VMs might fail due to insufficient file handles. Such VMs might need more than the default limit of 2048 handles.

Workaround: Apply the VM configuration setting `vmiop.maxFileHandles = 16384`.

Known Issues from Previous Releases

For a list of known issues from previous releases, see VMware ESXi 7.0 Update 3n Release Notes.

VMware ESXi 7.0 Update 3n Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues from Previous Releases

Introduction

ESXi 7.0 Update 3n | JUL 06 2023 | Build 21930508 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3n, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3n. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- ESXi 7.0 Update 3n delivers bug fixes documented in the Resolved Issues section.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3m Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3l Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes

- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Patches Contained in This Release

This release of ESXi 7.0 Update 3n delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3n-21930508-depot.zip
Build:	21930508
Download Size:	379.4 MB
md5sum:	0aa019e1a54fd113a415daea5038351a
sha256checksum:	189a5a11849bcfabc4d8ae54ee8246f5f86d31eb3164efc3c76613a31b7be467
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.95.21930508	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.95.21930508	Bugfix	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The **ESXi** and **esx-update** bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity
ESXi70U3n-21930508	Bugfix	Critical

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3n-21930508-standard
ESXi-7.0U3n-21930508-no-tools

ESXi Image

Name and Version	Release Date	Category	Detail
ESXi70U3n-21930508	JUL 06 2023	Bugfix	Bugfix image

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

ESXi_7.0.3-0.95.21930508

Patch Category	Bugfix

Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-base_7.0.3-0.95.21930508 • VMware_bootbank_trx_7.0.3-0.95.21930508 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.95.21930508 • VMware_bootbank_vdfs_7.0.3-0.95.21930508 • VMware_bootbank_esxio-combiner_7.0.3-0.95.21930508 • VMware_bootbank_cpu-microcode_7.0.3-0.95.21930508 • VMware_bootbank_esx-xserver_7.0.3-0.95.21930508 • VMware_bootbank_vsan_7.0.3-0.95.21930508 • VMware_bootbank_native-misc-drivers_7.0.3-0.95.21930508 • VMware_bootbank_vsanhealth_7.0.3-0.95.21930508 • VMware_bootbank_gc_7.0.3-0.95.21930508 • VMware_bootbank_bmcal_7.0.3-0.95.21930508 • VMware_bootbank_crx_7.0.3-0.95.21930508
PRs Fixed	3192477, 3186367
CVE numbers	N/A

This patch updates the **esx-base** VIB. Due to their dependency with the **esx-base** VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: **trx, esx-dvfilter-generic-fastpath, vdfs, esxio-combiner, cpu-microcode, esx-xserver, vsan, native-misc-drivers, vsanhealth, gc, bmcal** and **crx**. This patch resolves the following issues:

- **PR 3192477: Many LRO-capable PNICs do not aggregate packets from overlay traffic**
  Many physical networks adaptors (PNICs) that have the Hardware Large Receive Offload (LRO) capability might not aggregate packets from the Generic Network Virtualization Encapsulation (Geneve) overlay traffic.
  This issue is resolved in this release. The fix adds a software-based LRO functionality within the VMkernel that makes sure that if an LRO-capable PNIC does not aggregate packets from the Geneve overlay traffic, the VMkernel aggregates them instead. The change does not affect VLAN and VXLAN traffic.
- **PR 3186367: If virtual machines connected to an NSX logical switch stay on an ESXi host during a host reboot, such VMs might lose connectivity**
  If virtual machines connected to an NSX logical switch are not migrated and remain on an ESXi host during a host reboot, the VNICs of such VMs might lose connectivity.
  This issue is resolved in this release.

esx-update_7.0.3-0.95.21930508

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-update_7.0.3-0.95.21930508

	• VMware_bootbank_loadesx_7.0.3-0.95.21930508
PRs Fixed	N/A
CVE numbers	N/A

Due to their dependency with the **esx-base** VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: **loadesx** and **esx-update**.

ESXi-7.0U3n-21930508-standard

Profile Name	ESXi-7.0U3n-21930508-standard
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	July 06, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-base_7.0.3-0.95.21930508 • VMware_bootbank_trx_7.0.3-0.95.21930508 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.95.21930508 • VMware_bootbank_vdfs_7.0.3-0.95.21930508 • VMware_bootbank_esxio-combiner_7.0.3-0.95.21930508 • VMware_bootbank_cpu-microcode_7.0.3-0.95.21930508 • VMware_bootbank_esx-xserver_7.0.3-0.95.21930508 • VMware_bootbank_vsan_7.0.3-0.95.21930508 • VMware_bootbank_native-misc-drivers_7.0.3-0.95.21930508 • VMware_bootbank_vsanhealth_7.0.3-0.95.21930508 • VMware_bootbank_gc_7.0.3-0.95.21930508 • VMware_bootbank_bmcal_7.0.3-0.95.21930508 • VMware_bootbank_crx_7.0.3-0.95.21930508 • VMware_bootbank_esx-update_7.0.3-0.95.21930508 • VMware_bootbank_loadesx_7.0.3-0.95.21930508
PRs Fixed	3192477, 3186367
Related CVE numbers	N/A

- **This patch resolves the following issues:**
  - Many physical networks adaptors (PNICs) that have the Hardware Large Receive Offload (LRO) capability might not aggregate packets from the Generic Network Virtualization Encapsulation (Geneve) overlay traffic.
  - If virtual machines connected to an NSX logical switch are not migrated and remain on an ESXi host during a host reboot, the VNICs of such VMs might lose connectivity.

ESXi-7.0U3n-21930508-no-tools

Profile Name	ESXi-7.0U3n-21930508-no-tools
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	July 06, 2023

Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-base_7.0.3-0.95.21930508 • VMware_bootbank_trx_7.0.3-0.95.21930508 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.95.21930508 • VMware_bootbank_vdfs_7.0.3-0.95.21930508 • VMware_bootbank_esxio-combiner_7.0.3-0.95.21930508 • VMware_bootbank_cpu-microcode_7.0.3-0.95.21930508 • VMware_bootbank_esx-xserver_7.0.3-0.95.21930508 • VMware_bootbank_vsan_7.0.3-0.95.21930508 • VMware_bootbank_native-misc-drivers_7.0.3-0.95.21930508 • VMware_bootbank_vsanhealth_7.0.3-0.95.21930508 • VMware_bootbank_gc_7.0.3-0.95.21930508 • VMware_bootbank_bmcal_7.0.3-0.95.21930508 • VMware_bootbank_crx_7.0.3-0.95.21930508 • VMware_bootbank_esx-update_7.0.3-0.95.21930508 • VMware_bootbank_loadesx_7.0.3-0.95.21930508
PRs Fixed	3192477, 3186367
Related CVE numbers	N/A

- **This patch resolves the following issues:**
  - Many physical networks adaptors (PNICs) that have the Hardware Large Receive Offload (LRO) capability might not aggregate packets from the Generic Network Virtualization Encapsulation (Geneve) overlay traffic.
  - If virtual machines connected to an NSX logical switch are not migrated and remain on an ESXi host during a host reboot, the VNICs of such VMs might lose connectivity.

ESXi70U3n-21930508

Name	ESXi
Version	ESXi70U3n-21930508
Release Date	July 06, 2023
Category	Bugfix
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component
PRs Fixed	3192477, 3186367
Related CVE numbers	N/A

Known Issues from Previous Releases

The earlier known issues are grouped as follows.

- vSAN Issues
- vSphere Cluster Services Issues
- Installation, Upgrade, and Migration Issues
- Security Features Issues
- Networking Issues
- Storage Issues

- vCenter Server and vSphere Client Issues
- Virtual Machine Management Issues
- vSphere HA and Fault Tolerance Issues
- vSphere Lifecycle Manager Issues
- Miscellaneous Issues
- vSphere Client Issues

vSAN Issues

If you change the preferred site in a VMware vSAN Stretched Cluster, some objects might incorrectly appear as compliant

If you change the preferred site in a stretched cluster, some objects might incorrectly appear as compliant, because their policy settings might not automatically change. For example, if you configure a virtual machine to keep data at the preferred site, when you change the preferred site, data might remain on the nonpreferred site.

Workaround: Before you change a preferred site, in Advanced Settings, lower the `ClomMaxCrawlCycleMinutes` setting to 15 min to make sure objects policies are updated. After the change, revert the `ClomMaxCrawlCycleMinutes` option to the earlier value.

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the
requirement cannot be satisfied within the ImageProfile. Please refer to the log file for
more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s).`

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU.`

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer.`

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Set-VMHostService -policy "off"$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx`, the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1`.

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set --tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer": { "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"`, run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`

Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
`./opt/likewise/bin/lw-update-dns`
Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo`"

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo`"

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.

4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command:
   `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command:
   `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command:
   `esxcli network firewall load.`
5. Start the hostd service by using the command:
   `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats`, you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835`.

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0`.

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set` **-o** `/USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.
2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

VMware ESXi 7.0 Update 3m Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Patches Contained in This Release
- Patch Download and Installation
- Resolved Issues
- Known Issues from Previous Releases

Introduction

ESXi 7.0 Update 3m | MAY 03 2023 | Build 21686933 Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3m, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3m. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- ESXi 7.0 Update 3m resolves issues about ESXi hosts losing network connectivity in certain environments and under specific conditions. For more information, see VMware knowledge base articles 91887 and 92035, and the Resolved Issues section.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3l Release Notes

- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Patches Contained in This Release

This release of ESXi 7.0 Update 3m delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3m-21686933-depot.zip
Build:	21686933
Download Size:	379.4 MB
md5sum:	9cd52571752b939637f80b351daace94
sha256checksum:	8c7892af03254259db28e7f2982be2802dcf66bdb2fc92e15a06fe7e7835b692
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.90.21686933	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.90.21686933	Bugfix	Critical
Broadcom NetXtreme I ESX VMKAPI ethernet driver	Broadcom-ntg3_4.1.9.0-5vmw.703.0.90.21686933	Bugfix	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include all of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity
ESXi70U3m-21686933	Bugfix	Critical

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3m-21686933-standard
ESXi-7.0U3m-21686933-no-tools

ESXi Image

Name and Version	Release Date	Category	Detail
ESXi70U3m-21686933	MAY 03 2023	Bugfix	Bugfix image

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Resolved Issues

ESXi_7.0.3-0.90.21686933

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.90.21686933 • VMware_bootbank_esx-base_7.0.3-0.90.21686933 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.90.21686933 • VMware_bootbank_native-misc-drivers_7.0.3-0.90.21686933 • VMware_bootbank_bmcal_7.0.3-0.90.21686933 • VMware_bootbank_esx-xserver_7.0.3-0.90.21686933 • VMware_bootbank_vsanhealth_7.0.3-0.90.21686933 • VMware_bootbank_vdfs_7.0.3-0.90.21686933 • VMware_bootbank_cpu-microcode_7.0.3-0.90.21686933 • VMware_bootbank_vsan_7.0.3-0.90.21686933 • VMware_bootbank_esxio-combiner_7.0.3-0.90.21686933 • VMware_bootbank_crx_7.0.3-0.90.21686933 • VMware_bootbank_trx_7.0.3-0.90.21686933
PRs Fixed	3164897
CVE numbers	N/A

This patch updates the **esx-base** VIB. Due to their dependency with the **esx-base** VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: **gc, esx-dvfilter-generic-fastpath, native-misc-drivers, bmcal, esx-xserver, vsanhealth, vdfs, cpu-microcode, vsan, esxio-combiner, crx,** and **trx**. This patch resolves the following issue:

- **PR 3164897: After an upgrade to ESXi 7.0 Update 3l, some ESXi hosts and virtual machines connected to virtual switches might lose network**
  After an upgrade to ESXi 7.0 Update 3l, some ESXi hosts, their VMs, and other VMkernel ports, such as ports used by vSAN and vSphere Replication, which are connected to virtual switches, might lose connectivity due to an unexpected change in the NIC teaming policy. For example, the teaming policy on a portgroup might change to **Route Based on Originating Virtual Port** from **Route Based on IP Hash**. As a result, such a portgroup might lose network connectivity and some ESXi hosts and their VMs become inaccessible.
  This issue is resolved in this release.

esx-update_7.0.3-0.90.21686933

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.90.21686933

	• VMware_bootbank_esx-update_7.0.3-0.90.21686933
PRs Fixed	N/A
CVE numbers	N/A

Due to their dependency with the **esx-base** VIB, the following VIBs are updated with build number and patch version changes, but deliver no fixes: **loadesx** and **esx-update**.

Broadcom-ntg3_4.1.9.0-5vmw.703.0.90.21686933

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_ntg3_4.1.9.0-5vmw.703.0.90.21686933
PRs Fixed	3182870
CVE numbers	N/A

Updates the **ntg3** VIB to resolve the following issue:

- **PR 3182870: After upgrading the ntg3 driver to version 4.1.9.0-4vmw, Broadcom NICs with fiber physical connectivity might lose network**
  Changes in the **ntg3** driver version **4.1.9.0-4vmw** might cause link issues for the fiber physical layer and connectivity on some NICs, such as Broadcom 1Gb, fails to come up.
  This issue is resolved in this release. ESXi 7.0 Update 3m provides **ntg3** driver version **4.1.9.0-5vmw**. The fix also adds a module parameter, **fifoElastic**, which you can enable in case of jumbo frame drops in certain Dell switches. To enable the parameter, use the following command:
  esxcli system module parameters set -p 'fifoElastic=1' -m ntg3

ESXi-7.0U3m-21686933-standard

Profile Name	ESXi-7.0U3m-21686933-standard
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	May 03, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.90.21686933 • VMware_bootbank_esx-base_7.0.3-0.90.21686933 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.90.21686933 • VMware_bootbank_native-misc-drivers_7.0.3-0.90.21686933 • VMware_bootbank_bmcal_7.0.3-0.90.21686933 • VMware_bootbank_esx-xserver_7.0.3-0.90.21686933 • VMware_bootbank_vsanhealth_7.0.3-0.90.21686933

	• VMware_bootbank_vdfs_7.0.3-0.90.21686933 • VMware_bootbank_cpu-microcode_7.0.3-0.90.21686933 • VMware_bootbank_vsan_7.0.3-0.90.21686933 • VMware_bootbank_esxio-combiner_7.0.3-0.90.21686933 • VMware_bootbank_crx_7.0.3-0.90.21686933 • VMware_bootbank_trx_7.0.3-0.90.21686933 • VMware_bootbank_loadesx_7.0.3-0.90.21686933 • VMware_bootbank_esx-update_7.0.3-0.90.21686933 • VMW_bootbank_ntg3_4.1.9.0-5vmw.703.0.90.21686933
PRs Fixed	3164897, 3182870
Related CVE numbers	N/A

- **This patch resolves the following issues:**
  - After an upgrade to ESXi 7.0 Update 3l, some ESXi hosts, their VMs, and other VMkernel ports, such as ports used by vSAN and vSphere Replication, which are connected to virtual switches, might lose connectivity due to an unexpected change in the NIC teaming policy. For example, the teaming policy on a portgroup might change to **Route Based on Originating Virtual Port** from **Route Based on IP Hash**. As a result, such a portgroup might lose network connectivity and some ESXi hosts and their VMs become inaccessible.
  - Changes in the **ntg3** driver version 4.1.9.0-4vmw might cause link issues for the fiber physical layer and connectivity on some NICs, such as Broadcom 1Gb, fails to come up.

ESXi-7.0U3m-21686933-no-tools

Profile Name	ESXi-7.0U3m-21686933-no-tools
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	May 03, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_gc_7.0.3-0.90.21686933 • VMware_bootbank_esx-base_7.0.3-0.90.21686933 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.90.21686933 • VMware_bootbank_native-misc-drivers_7.0.3-0.90.21686933 • VMware_bootbank_bmcal_7.0.3-0.90.21686933 • VMware_bootbank_esx-xserver_7.0.3-0.90.21686933 • VMware_bootbank_vsanhealth_7.0.3-0.90.21686933 • VMware_bootbank_vdfs_7.0.3-0.90.21686933 • VMware_bootbank_cpu-microcode_7.0.3-0.90.21686933 • VMware_bootbank_vsan_7.0.3-0.90.21686933 • VMware_bootbank_esxio-combiner_7.0.3-0.90.21686933 • VMware_bootbank_crx_7.0.3-0.90.21686933 • VMware_bootbank_trx_7.0.3-0.90.21686933 • VMware_bootbank_loadesx_7.0.3-0.90.21686933 • VMware_bootbank_esx-update_7.0.3-0.90.21686933 • VMW_bootbank_ntg3_4.1.9.0-5vmw.703.0.90.21686933
PRs Fixed	3164897, 3182870
Related CVE numbers	N/A

- **This patch resolves the following issues:**
  - After an upgrade to ESXi 7.0 Update 3l, some ESXi hosts, their VMs, and other VMkernel ports, such as ports used by vSAN and vSphere Replication, which are connected to virtual switches, might lose connectivity due to an unexpected change in the NIC teaming policy. For example, the teaming policy on a portgroup might change to **Route Based on Originating Virtual Port** from **Route Based on IP Hash**. As a result, such a portgroup might lose network connectivity and some ESXi hosts and their VMs become inaccessible.
  - Changes in the **ntg3** driver version 4.1.9.0-4vmw might cause link issues for the fiber physical layer and connectivity on some NICs, such as Broadcom 1Gb, fails to come up.

ESXi70U3m-21686933

Name	ESXi
Version	ESXi70U3m-21686933
Release Date	May 03, 2023
Category	Bugfix
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • Broadcom NetXtreme I ESX VMKAPI ethernet driver
PRs Fixed	3164897, 3182870
Related CVE numbers	N/A

Known Issues from Previous Releases

The earlier known issues are grouped as follows.

- vSAN Issues
- vSphere Cluster Services Issues
- Installation, Upgrade, and Migration Issues
- Security Features Issues
- Networking Issues
- Storage Issues
- vCenter Server and vSphere Client Issues
- Virtual Machine Management Issues
- vSphere HA and Fault Tolerance Issues
- vSphere Lifecycle Manager Issues
- Miscellaneous Issues
- vSphere Client Issues

vSAN Issues

If you change the preferred site in a VMware vSAN Stretched Cluster, some objects might incorrectly appear as compliant

If you change the preferred site in a stretched cluster, some objects might incorrectly appear as compliant, because their policy settings might not automatically change. For example, if you configure a virtual machine to keep data at the preferred site, when you change the preferred site, data might remain on the nonpreferred site.

Workaround: Before you change a preferred site, in Advanced Settings, lower the `ClomMaxCrawlCycleMinutes` setting to 15 min to make sure objects policies are updated. After the change, revert the `ClomMaxCrawlCycleMinutes` option to the earlier value.

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the requirement cannot be satisfied within the ImageProfile. Please refer to the log file for more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s)`.

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU`.

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer`.

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.

2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Set-VMHostService -policy "off"$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx`, the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1`.

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set --tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer":
{ "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"` , run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error`. The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command:
   `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command:
   `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command:
   `esxcli network firewall load.`
5. Start the hostd service by using the command:
   `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats` , you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835` .

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0` .

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set` **-o** `/USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.
2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

VMware ESXi 7.0 Update 3l Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of ESXi 7.0
- Patches Contained in This Release
- Patch Download and Installation

- Product Support Notices
- Resolved Issues
- Known Issues
- Known Issues from Previous Releases

Introduction

ESXi 7.0 Update 3l | MAR 30 2023 | ISO Build 21424296
Check for additions and updates to these release notes.

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3l, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3l. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- ESXi 7.0 Update 3l supports vSphere Quick Boot on the following servers:
  - Cisco
    - UCSC-C225-M6S
  - Dell
    - R660 vSAN Ready Node
    - R760 vSAN Ready Node
    - PowerEdge R660xs
    - PowerEdge R760xa
    - PowerEdge R760xd2
    - PowerEdge R760xs
    - PowerEdge R860
    - PowerEdge R960
    - PowerEdge T560
  - HPE
    - Alletra 4120
    - Cray XD220v
    - ProLiant DL320 Gen11
    - ProLiant DL380a Gen11
    - ProLiant DL560 Gen11
    - ProLiant ML110 Gen11
- This release resolves CVE-2023-1017. VMware has evaluated the severity of this issue to be in the low severity range with a maximum CVSSv3 base score of 3.3.
- This release resolves CVE-2023-1018. VMware has evaluated the severity of this issue to be in the low severity range with a maximum CVSSv3 base score of 3.3.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3k Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3j Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3i Release Notes

- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Patches Contained in This Release

This release of ESXi 7.0 Update 3l delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3l-21424296-depot
Build:	21424296
Download Size:	570.6 MB
md5sum:	bc8be7994ff95cf45e218f19eb38a4f1
sha256checksum:	a85acc0fab15d5c2744e6b697817961fde3979eddfc4dd1af07c83731f2f87cf
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.85.21424296	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.85.21424296	Bugfix	Critical
Broadcom NetXtreme I ESX VMKAPI ethernet driver	Broadcom-ntg3_4.1.9.0-4vmw.703.0.85.21424296	Bugfix	Critical
Non-Volatile memory controller driver	VMware-NVMe-PCIe_1.2.3.16-2vmw.703.0.85.21424296	Bugfix	Critical
USB Native Driver for VMware	VMware-vmkusb_0.1-8vmw.703.0.85.21424296	Bugfix	Critical

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.80.21422485	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.80.21422485	Security	Critical
ESXi Tools Component	VMware-VM-Tools_12.1.5.20735119-21422485	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Details
ESXi70U3l-21424296	Bugfix	Critical	Security and Bugfix
ESXi70U3sl-21422485	Security	Critical	Security only

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-7.0U3l-21424296-standard
ESXi-7.0U3l-21424296-no-tools
ESXi-7.0U3sl-21422485-standard
ESXi-7.0U3sl-21422485-no-tools

ESXi Image

Name and Version	Release Date	Category	Detail
ESXi7.0U3l - 21424296	MAR 30 2023	Bugfix	Security and Bugfix image
ESXi7.0U3sl - 21422485	MAR 30 2023	Security	Security only image

Patch Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.

The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.

You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle ZIP file.

For details, see Upgrading Hosts by Using ESXCLI Commands, and the VMware ESXi Upgrade guide.

Product Support Notices

- **Restoring Memory Snapshots of a VM with independent disk for virtual machine backups is not supported**: You can take a memory snapshot of a virtual machine with an independent disk only to analyze the guest operating system behavior of a virtual machine. You cannot use such snapshots for virtual machine backups because restoring this type of snapshots is unsupported. You can convert a memory snapshot to a powered-off snapshot, which can be successfully restored.

Resolved Issues

The resolved issues are grouped as follows.

- ESXi_7.0.3-0.85.21424296
- esx-update_7.0.3-0.85.21424296
- Broadcom-ntg3_4.1.9.0-4vmw.703.0.85.21424296
- VMware-vmkusb_0.1-8vmw.703.0.85.21424296
- VMware-NVMe-PCIe_1.2.3.16-2vmw.703.0.85.21424296
- ESXi_7.0.3-0.80.21422485
- esx-update_7.0.3-0.80.21422485
- VMware-VM-Tools_12.1.5.20735119-21422485
- ESXi-7.0U3l-21424296-standard
- ESXi-7.0U3l-21424296-no-tools
- ESXi-7.0U3l-21422485-standard
- ESXi-7.0U3l-21422485-no-tools
- ESXi70U3l-21424296
- ESXi70U3sl-21422485

ESXi_7.0.3-0.85.21424296

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs Included	• VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.85.21424296 • VMware_bootbank_vsan_7.0.3-0.85.21424296

	• VMware_bootbank_bmcal_7.0.3-0.85.21424296 • VMware_bootbank_crx_7.0.3-0.85.21424296 • VMware_bootbank_esx-ui_2.9.2-21141530 • VMware_bootbank_esxio-combiner_7.0.3-0.85.21424296 • VMware_bootbank_vsanhealth_7.0.3-0.85.21424296 • VMware_bootbank_native-misc-drivers_7.0.3-0.85.21424296 • VMware_bootbank_gc_7.0.3-0.85.21424296 • VMware_bootbank_cpu-microcode_7.0.3-0.85.21424296 • VMware_bootbank_vdfs_7.0.3-0.85.21424296 • VMware_bootbank_esx-xserver_7.0.3-0.85.21424296 • VMware_bootbank_esx-base_7.0.3-0.85.21424296 • VMware_bootbank_trx_7.0.3-0.85.21424296
PRs Fixed	3057026, 3062185, 3040049, 3061156, 3023389, 3062861, 3089449, 3081870, 3082900, 3033157, 3090683, 3075786, 3074392, 3081275, 3080022, 3083314, 3084812, 3074360, 3092270, 3076977, 3051685, 3082477, 3082282, 3082427, 3077163, 3087219, 3074187, 3082431, 3050562, 3072430, 3077072, 3077060, 3046875, 3082991, 3083473, 3051059, 3091256, 3074912, 3058993, 3063987, 3072500, 3060661, 3076188, 3049652, 2902475, 3087946, 3116848, 3010502, 3118090, 3078875, 3069298, 3074121
CVE numbers	CVE-2023-1017, CVE-2023-1018

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `esx-dvfilter-generic-fastpath`, `vsan`, `bmcal`, `crx`, `esx-ui`, `esxio-combiner`, `vsanhealth`, `native-misc-drivers`, `gc`, `cpu-microcode`, `vdfs`, `esx-xserver`, `esx-base`, and `trx` VIBs to resolve the following issues:

- **PR 3057026: When you change the NUMA nodes Per Socket (NPS) setting on an AMD EPYC 9004 'Genoa' server from the default of 1, you might see incorrect number of sockets**
  In the vSphere Client and the ESXi Host Client, you might see incorrect number of sockets and respectively cores per socket when you change the NPS setting on an AMD EPYC 9004 server from the default of 1, or Auto, to another value, such as 2 or 4.
  This issue is resolved in this release.
- **PR 3062185: ESXi hosts might fail with a purple diagnostic screen during a vSphere Storage vMotion operation or hot-adding a device**
  Due to a rare race condition during a Fast Suspend Resume (FSR) operation on a VM with shared pages between VMs, ESXi hosts might fail with a purple diagnostic screen with an error such as **PFrame_IsBackedByLPage** in the backtrace. The issue occurs during vSphere Storage vMotion operations or hot-adding a device.
  This issue is resolved in this release.
- **PR 3040049: The performance of the pktcap-uw utility degrades when using the -c option for counting packets in heavy network traffic**
  Packet capture with the **-c** option of the **pktcap-uw** utlity in heavy network traffic might be slower than packet capture without the option. You might also see a delay in capturing packets, so that the last package counted has a timestap few seconds earlier than the stop time of the function. The issue results from the **File_GetSize** function to check file sizes, which is slow in VMFS environments and causes low performance of **pktcap-uw**.
  This issue is resolved in this release. The fix changes the **File_GetSize** function with the **lseek** function to enhance performance.

- **PR 3061156: The Data Center Bridging (DCB) daemon on an ESXi host might generate a log spew in the syslog**
  In the **syslog** file you might see frequent log messages such as:
  2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] * Received pre-CEE DCBX Packet on port: vmnicX**
  2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info]2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Src MAC: xc:xc:X0:0X:xc:xx
  2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Dest MAC: X0:xb:xb:fx:0X:X1
  2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] 2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Port ID TLV:
  2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] ifName:
  The issue occurs because the Data Center Bridging (DCB) daemon, **dcbd**, on the ESXi host records unnecessary messages at **/var/log/syslog.log**. As a result, the log file might quickly fill up with **dcbd** logs.
  This issue is resolved in this release.
- **PR 3023389: You see up to 100% CPU usage on one of the cores of an ESXi host due to an early timed-wait system call**
  In some cases, a timed-wait system call in the VMkernel might return too early. As a result, some applications, such as the System Health Agent, might take up to 100% of the CPU usage on one of the ESXi host cores.
  This issue is resolved in this release.
- **PR 3062861: You do not see virtual machine image details in the Summary tab of the vSphere Client**
  Due to an issue with the IPv6 loopback interfaces, you might not see virtual machine image details in the **Summary** tab of the vSphere Client.
  This issue is resolved in this release.
- **PR 3089449: If the number of paths from an ESXi host using SATP ALUA to storage exceeds 255, you might see I/O latency in some VMs**
  If the number of paths from an ESXi host using NMP SATP ALUA to storage exceed 255, ESXi ignores part of the ALUA information reported by the target and incorrectly retains some of the path state as active optimised. As a result, some I/Os use the non-optimised path to the storage device and cause latency issues..
  This issue is resolved in this release. The fix makes sure that when RTPG response length is greater than pre-allocated buffer length, ESXi reallocates RTPG buffer with the required size and re-issues the RTPG command.
- **PR 3081870: ESXi host reboot process stops with “initializing init_VMKernelShutdownHelper: (14/39) ShutdownSCSICleanupForDevTearDown” message**
  In some cases, during an ESXi host shutdown, helper queues of device probe requests get deleted, but the reference to the device remains. As a result, the ESXi host reboot stops with a message such as **initializing init_VMKernelShutdownHelper: (14/39) ShutdownSCSICleanupForDevTearDown** in the Direct Console User Interface (DCUI).
  This issue is resolved in this release. The fix adds a cancel function associated with helper requests that decrement device references when deleting helper queue requests.
- **PR 3082900: ESXi hosts might fail with a purple diagnostic screen during a VM Instant Clone operation**
  Due to a race condition during an Instant Clone operation, VM memory pages might be corrupted and the ESXi host might fail with a purple diagnostic screen. You see errors such as **VmMemMigrate_MarkPagesCow** or **AsyncRemapProcessVMRemapList** in the backtrace.
  This issue is resolved in this release.
- **PR 3033157: Storage failover might take long as repeated scans may be required to bring all paths to a LUN online**
  In some environments with SATP plug-ins such as **satp_alua** and **satp_alua_cx**, bringing all paths to a LUN online might require several scans. As a result, a storage failover operation might take long. For example, with 4 paths to a LUN, it might take up to 20 minutes to bring the 4 paths online.
  This issue is resolved in this release.

- **PR 3090683: Virtual machine vSphere tags might be lost after vSphere vMotion operations across vCenter Server instances**
  After vSphere vMotion operations across vCenter Server instances for VMs that have vSphere tags, it is possible that the tags do not exist in the target location. The issue only occurs in migration operations between vCenter Server instances that do not share storage.
  This issue is resolved in this release.
- **PR 3075786: The multicast filter mode of an NSX Virtual Switch might intermittently revert from legacy to snooping**
  When you set the multicast filter mode of an NSX Virtual Switch for NVDS, the mode might intermittently revert from legacy to snooping.
  This issue is resolved in this release. If you already face the issue, clear the stale property on the NVDS by completing the following steps:
  a. Run the **net-dvs** command on the ESXi host and check if **com.vmware.etherswitch.multicastFilter** is set on the NVDS. If **com.vmware.etherswitch.multicastFilter** is not set, no additional steps are required.
  b. If the property **com.vmware.etherswitch.multicastFilter** is set, use the following command to clear it:
  net-dvs -u com.vmware.etherswitch.multicastFilter -p globalPropList <NVDS name>
- **PR 3074392: IOFilterVP service stops when you run a Nessus scan on an ESXi host**
  When you run a Nessus scan, which internally runs a SYN scan, to detect active ports on an ESXi host, the iofiltervpd service might shut down. The service cannot be restarted within the max retry attempts due to the SYN scan.
  This issue is resolved in this release. The fix makes sure the IOFilterVP service handles the possible connection failure due to SYN scans.
- **PR 3081275: You see no change in the ESXi config after you run a restore config procedure and the ESXi host reboots**
  If a VIB containing a new kernel module is installed before you run any of the restore config procedures described in VMware knowledge base article 2042141, you see no change in the config after the ESXi host reboots. For example, if you attempt to restore the ESXi config immediately after installing the NSX VIB, the ESXi host reboots, but no changes in the config are visible. The issue occurs due to a logical fault in the updates of the bootbank partition used for ESXi host reboots after a new kernel module VIB is installed.
  This issue is resolved in this release.
- **PR 3080022: Listing files on mounted NFS 4.1 Azure storage might not work as expected**
  Listing files of mounted NFS 4.1 Azure storage might not work as expected, because although the files exist and you can open them by name, the **ls** command on an ESXi host by using SSH does not show any files.
  This issue is resolved in this release.
- **PR 3083314: Network File Copy (NFC) properties in the vpxa.cfg file might cause an ESXi host to fail with a purple diagnostic screen during upgrade**
  Starting with ESXi 7.0 Update 1, the **vpxa.cfg** file no longer exists and the vpxa configuration belongs to the ESXi Configuration Store (**ConfigStore**). When you upgrade an ESXi host from a version earlier than 7.0 Update 1 to a later version, the fields **Vpx.Vpxa.config.nfc.loglevel** and **Vpx.Vpxa.config.httpNfc.accessMode** in the **vpxa.cfg** file might cause the ESXi host to fail with a purple diagnostic screen during the conversion from **vpxa.cfg** format to **ConfigStore** format. The issue occurs due to discrepancies in the NFC log level between **vpxa.cfg** and **ConfigStore**, and case-sensitive values.
  This issue is resolved in this release. The fix removes the strict case-sensitive rules and maps NFC log level with their **ConfigStore** equivalents. For more information, see VMware knowledge base article 90865.
- **PR 3084812: Virtual machines might take longer to respond or become temporary unresponsive when vSphere DRS triggers multiple migration operations**
  In rare cases, multiple concurrent open and close operations on datastores, for example when vSphere DRS triggers multiple migration tasks, might cause some VMs to take longer to complete in-flight disk I/Os. As a result, such virtual machines might take longer to respond or become unresponsive for a short time. The issue is more likely to occur on VMs that have multiple virtual disks over different datastores.
  This issue is resolved in this release.

- **PR 3074360: After an API call to reload a virtual machine, the VM virtual NIC might disconnect from a Logical Switch Port (LSP)**
  During an API call to reload a virtual machine from one ESXi host to another, the **externalId** in the VM port data file might be lost. As a result, after the VM reloads, the VM virtual NIC might not be able to connect to a LSP.
  This issue is resolved in this release.
- **PR 3092270: VMware Host Client fails to attach an existing virtual disk to a virtual machine**
  After upgrading to ESXi 7.0 Update 3i, you might not be able to attach an existing virtual machine disk (VMDK) to a VM by using the VMware Host Client, which is used to connect to and manage single ESXi hosts. The issue does not affect the vSphere Client.
  This issue is resolved in this release.
- **PR 3076977: ESXi host might fail with a purple diagnostic screen due to a rare issue with dereferencing a freed pointer**
  Due to a race condition between the Create and Delete resource pool workflows, a freed pointer in the VMFS resource pool cache might get dereferenced. As a result, ESXi hosts might fail with a purple diagnostic screen and error such as:
  @BlueScreen: #PF Exception 14 in world 2105491:res3HelperQu IP 0x420032a21f55 addr 0x0
  This issue is resolved in this release.
- **PR 3051685: The batch QueryUnresolvedVmfsVolume API might take long to list a large number of unresolved VMFS volumes**
  With the batch **QueryUnresolvedVmfsVolume** API, you can query and list unresolved VMFS volumes or LUN snapshots. You can then use other batch APIs to perform operations, such as re-signaturing specific unresolved VMFS volumes. By default, when the API **QueryUnresolvedVmfsVolume** is invoked on a host, the system performs an additional filesystem liveness check for all unresolved volumes that are found. The liveness check detects whether the specified LUN is mounted on other hosts, whether an active VMFS heartbeat is in progress, or if there is any filesystem activity. This operation is time consuming and requires at least 16 seconds per LUN. As a result, when your environment has a large number of snapshot LUNs, the query and listing operation might take significant time.
  This issue is resolved in this release.
- **PR 3082477: vSAN cluster shutdown fails with error: 'NoneType' object has no attribute '_mold'**
  This problem can occur when vCenter manages multiple clusters, and the vCenter VM runs on one of the clusters. If you shut down the cluster where the vCenter VM resides, the following error can occur during the shutdown operation: **'NoneType' object has no attribute '_mold'**. The vCenter VM is not powered off.
  This issue is resolved in this release.
- **PR 3082282: You do not see the Restart Cluster option in the vSphere Client after shutting down multiple vSAN clusters**
  This problem can occur when vCenter manages multiple clusters and runs several shut down and restart cluster operations in parallel. For example, if you shut down 3 clusters and restart the vSAN health service or the vCenter VM, and you restart one of the 3 clusters before the others, the **Restart Cluster** option might be available for the first vSAN cluster, but not for the other clusters.
  This issue is resolved in this release.
- **PR 3082427: You see an unexpected time drift alert on vSAN clusters managed by the same vCenter Server**
  Unexpected time drift can occur intermittently on a vSAN cluster when a single vCenter Server manages several vSAN clusters, due to internal delays in VPXA requests. In the vSphere Client, in the vSAN Health tab, you see the status of **Time is synchronized across hosts and VC** changing from green to yellow and back to green.
  This issue is resolved in this release.
- **PR 3077163: When the ToolsRamdisk advanced option is active on an ESXi host, after a VM Tools upgrade, new versions are not available for VMs**
  When you enable the **ToolsRamdisk** advanced option that makes sure the **/vmtools** partition is always on a RAM disk rather than on a USB or SD-card, installing or updating the **tools-light** VIB does not update the content of the RAM

disk automatically. Instead, you must reboot the host so that the RAM disk updates and the new VM Tools version is available for the VMs.

This issue is resolved in this release. The fix makes sure that when **ToolsRamdisk** is enabled, VM Tools updates automatically, without the need of manual steps or restart.

- **PR 3087219: ESXi hosts might fail with a purple diagnostic screen after a migration operation**

  A rare race condition caused by memory reclamation for some performance optimization processes in vSphere vMotion might cause ESXi hosts to fail with a purple diagnostic screen.

  This issue is resolved in this release.
- **PR 3074187: ESXi hosts randomly fail with a purple diagnostic screen and an error such as Exception 14 in world #######**

  If your environment has both small and large file block clusters mapped to one affinity rule, when you add a cluster, the Affinity Manager might allocate more blocks for files than the actual volume of the datastore. As a result, ESXi hosts randomly fail with a purple diagnostic screen with error **Exception 14 in world #######**.

  This issue is resolved in this release.
- **PR 3082431: vSAN health history has no data available for the selected time period**

  This issue occurs when you view health details of any health check in the history view. In the vSphere Client, in the Skyline Health tab, you see a message such as **No data available for the selected time period**. The issue occurs when a query to the historical health records fails due to timestamps with an incorrect time zone.

  This issue is resolved in this release.
- **PR 3050562: You might see incorrect facility and severity values in ESXi syslog log messages**

  The logger command of some logger clients might not pass the right facility code to the ESXi syslog daemon and cause incorrect facility or severity values in ESXi syslog log messages.

  This issue is resolved in this release.
- **PR 3072430: A rare race condition in the Logical Volume Manager (LVM) schedule queue might cause an ESXi host to fail with a purple diagnostic screen**

  In rare cases, in a heavy workload, two LVM tasks that perform updating and querying on the device schedule in an ESXi host might run in parallel and cause a synchronization issue. As a result, the ESXi host might fail with a purple diagnostic screen and a messages similar to **LVMIoctlInt@com.vmware.lvm.ut#nover+0x1018 stack: 0xXXXXX and Addr3ResolvePhysVector@esx#nover+0x68 stack: 0xXXXX** in the backtrace.

  This issue is resolved in this release.
- **PR 3077072: When an ESXi host boots, some dynamically discovered iSCSI target portals and iSCSI LUNs might get deleted**

  In some cases, while an ESXi host boots, some dynamically discovered iSCSI targets might get deleted. As a result, after the boot completes, you might no longer see some iSCSI LUNs. The issue is more likely to occur in environments with Challenge-Handshake Authentication Protocol

  (CHAP) enabled for iSCSI.

  This issue is resolved in this release.
- **PR 3077060: The VMware Host Client or vSphere Client intermittently stop displaying software iSCSI adapters**

  In busy environments with many rescans by using a software iSCSI adapter, the VMware Host Client might intermittently stop displaying the adapter. The issue occurs only with target arrays which return target portals with both IPv4 and IPv6 addresses during discovery by using the **SendTargets** method.

  This issue is resolved in this release.
- **PR 3046875: Disabling Storage I/O Control on datastores results in high read I/O on all ESXi hosts**

  A rare issue with calculating the Max Queue Depth per datastore device might cause queue depth mismatch warnings from the underlying SCSI layer. As a result, when you disable Storage I/O Control on datastores, you might see high read I/O on all ESXi hosts.

  This issue is resolved in this release.

- **PR 3082991: After an upgrade to ESXi 7.0 Update 3 and later, you might see multiple -1.log files to fill up the root directory**
  Due to missing configuration for **stats-log** in the file **/etc/vmware/vvold/config.xml**, you might see multiple **-1.log** files to fill up the **/ramdisk** partition after an upgrade to ESXi 7.0 Update 3 and later.
  This issue is resolved in this release.
- **PR 3083473: Username or password in proxy cannot include an escape character**
  If a username or password in a network proxy contains any escape character, the environment fails to send network requests through the proxy.
  This issue is resolved in this release. The fix makes sure username or password work fine even with non-escaped characters.
- **PR 3051059: The command esxcli system ntp test fails to resolve the IP of an NTP server configured with additional parameters along with the host name**
  If you configure an NTP server on an ESXi host with additional parameters along with **hostname**, such as **min_poll** or **max_poll**, the command **esxcli system ntp test** might fail to resolve the IP address of that server. This issue occurs because in such configurations, the NTP name resolution applies to the entire server config instead of just the host name.
  This issue is resolved in this release.
- **PR 3091256: After upgrade to ESXi 7.0 Update 2 and later, VMs might not be able to communicate properly with some USB devices attached to the VMs**
  After upgrading to ESXi 7.0 Update 2 and later, a virtual machine might not discover some USB devices attached to it, such as an Eaton USB UPS, and fail to communicate with the device properly.
  This issue is resolved in this release.
- **PR 3074912: If you change the datastore of a cloned virtual machine before the initial power on, guest OS customizations might be lost**
  If you clone a VM, including the guest customization specs, move the VMDK file to another datastore and make it thick provisioned, and then power on the VM, the guest OS customization might not be preserved. In the hostd logs, you see an Event Type Description such as **The customization component failed to set the required parameters inside the guest operating system**.
  The issue occurs because while moving the VMDK file of the cloned VM to another datastore, the new **pathName** for the guest OS customization might temporarily be the same as the **oldPathName** and the package gets deleted.
  This issue is resolved in this release.
- **PR 3058993: Virtual machine-related tasks might fail when you use vSphere APIs for I/O Filtering (VAIO) for VMware or third-party backup applications**
  Improper sizing of the resource needs for the hostd service on an ESXi host might cause some virtual machine-related tasks to fail when you use vSphere APIs for I/O Filtering (VAIO) for VMware or third-party backup applications. For example, when a VAIO filter is attached to one or more virtual disks of a virtual machine, such VMs might fail to perform backups or power-on after a backup.
  This issue is resolved in this release. The fix increases the number of threads to prevent I/O-related issues with the hostd resources on ESXi hosts.
- **PR 3063987: First Class Disk (FCD) sync might fail on NFSv3 datastores and you see inconsistent values in Govc reports**
  A rare file corruption issue might occur when multiple ESXi hosts do a simultaneous file append operation on an NFSv3 datastore. As a result, if you use the Govc open source command-line utility to perform administrative actions on a vCenter instance, you might see reports with inconsistent values. For example, if you run the command **govc disk.ls** to list all FCDs in a newly created datastore, you see a different number of disks from what you expect.
  This issue is resolved in this release.
- **PR 3072500: ESXi hosts intermittently fail with a purple diagnostic screen and an error VERIFY bora/vmkernel/sched/cpusched.c**
  In rare cases, when a VMFS volume is closed immediately after it is opened, one of the threads in the opening process might race with a thread in the closing process and take a rare error handling path that can exit without unlocking a

locked spinlock. As a result, the ESXi host might fail with a purple diagnostic screen with a message in the backtrace such as: **@BlueScreen: VERIFY bora/vmkernel/sched/cpusched.c:11154.**

This issue is resolved in this release.

- **PR 3060661: Windows Server Failover Cluster (WSFC) applications might lose connectivity to a virtual volume-based disk after initiating a rebind operation on that disk**

  Due to reservation conflicts, WSFC applications might lose connectivity to a virtual volume-based disk after a rebind operation on that disk.

  This issue is resolved in this release.
- **PR 3076188: vSphere HA might not work as expected on a vSAN datastore after a power outage**

  In rare situations, the management agent that vSphere HA deploys on ESXi hosts, Fault Domain Manager (FDM), might fail to acquire a vSAN datastore in the first attempt before an exceptional condition, such as power outage, occurs. As a result, vSphere HA failover for virtual machines on that datastore might not be successful. In the vSphere Client, you see a message such as **This virtual machine failed to become vSphere HA Protected and HA may not attempt to restart it after a failure**. Successive attempts of FDM to acquire the vSAN datastore might also fail.

  This issue is resolved in this release. The fix makes sure that the successive attempts to acquire a vSAN datastore after an exceptional condition succeed.
- **PR 3049652: The Power|Total Energy (Wh) metric from the sustainability metrics in VMware vRealize Operations might display in wrong units**

  In the sustainability metrics in VMware vRealize Operations, you might see the value of **Power|Total Energy (Wh)** per virtual machine higher than the ESXi host on which the VM is hosted. The issue occurs because after measuring the total energy consumed by the VM, the **power.energy** performance counter is calculated and reported in millijoules instead of joules.

  This issue is resolved in this release.
- **PR 2902475: Windows virtual machines of hardware version 19 that have Virtualization-Based Security (VBS) enabled might fail with a blue diagnostic screen on ESXi hosts running on AMD processors**

  In ESXi hosts running on AMD processors, Windows virtual machines of hardware version 19 with VBS enabled might fail with a blue diagnostic screen due to a processor mode misconfiguration error. In the **vmware.log** file, you see errors such as **vcpu-0 - WinBSOD: Synthetic MSR[0xx0000x00] 0xxxx**.

  This issue is resolved in this release.
- **PR 3087946: vSphere Lifecycle Manager compliance scan might show a warning for a CPU that is supported**

  Due to an internal error, even if a CPU model is listed as supported in the VMware Compatibility Guide, in the vSphere Client you might see a warning such as **The CPU on the host is not supported by the image** during a compliance scan by using a vSphere Lifecycle Manager image. The warning does not prevent you from completing an update or upgrade.

  This issue is resolved in this release.
- **PR 3116848: Virtual machines with Virtualization-Based Security (VBS) enabled might fail with a blue diagnostic screen after a migration**

  When you migrate virtual machines with VBS enabled that reside on ESXi hosts running on AMD processors, such VMs might fail with a blue diagnostic screen on the target host due to a guest interruptibility state error.

  This issue is resolved in this release.
- **PR 3010502: If you override a networking policy for a port group and then revert the change, the override persists after an ESXi host reboot**

  When you override a networking policy such as Teaming, Security, or Shaping for a port group, and then revert the change, after a reboot of the ESXi host, you might still see the override setting. For example, if you accept promiscuous mode activation on a port group level, then revert the mode back to Reject, and reboot the ESXi host, the setting is still Accept.

  This issue is resolved in this release.

- **PR 3118090: The autocomplete attribute in forms for web access is not disabled on password and username fields**
  Your remote web server might contain an HTML form field that has an input of type **password** and **username** where the **autocomplete** attribute is not set to **off**. As a result, you might see a warning by security scanners such as **AutoComplete Attribute Not Disabled for Password in Form Based Authentication**. The setting of the **autocomplete** attribute to **on** does not directly put a risk on web servers, but in certain browsers, user credentials in such forms might be saved and potentially lead to a loss of confidentiality.
  This issue is resolved in this release. The fix makes sure the attribute **autocomplete** is set to **off** in password and username fields to prevent browsers from caching credentials.
- **PR 3078875: Cannot set IOPS limit for vSAN file service objects**
  vSAN Distributed File System (vDFS) objects do not support IOPS limit. You cannot set the IOPS limit for vSAN file service objects.
  This issue is resolved in this release. With the fix, you can set an IOPSLimit policy with vSAN file service objects.
- **PR 3069298: In vSphere Client, you do not see the asset tag for some servers**
  In vSphere Client, when you navigate to **Configure** > **Hardware** > **Overview**, for some servers you do not see any asset tag listed.
  This issue is resolved in this release. The fix ensures that vCenter receives either baseboard info (Type2) asset tag or chassis info(Type3) asset tag for the server. You see the chassis info asset tag when the baseboard info asset tag for the server is empty.
- **PR 3074121: Network configuration lost after vSAN upgrade to 7.0 or later**
  When you upgrade a vSAN host from a pre-6.2 release to 7.0 or later, the VMkernel port tagging for vSAN might be lost. If this occurs, vSAN networking configuration is missing after the upgrade.
  This issue is resolved in this release. The fix prevents the issue to occur on ESXi 7.0 Update 3l and later. If you already face the issue, upgrading to ESXi 7.0 Update 3l does not automatically resolve the issue, but you can manually fix it by enabling VMkernel traffic for vSAN on the ESXi host.
- **PR 3085003: Cannot enable vSAN File Service with uploaded OVF files**
  You cannot enable vSAN File Service if the vCenter does not have Internet access.
  This issue is resolved in this release.
- **PR 3088608: Virtual machines might fail with a core dump while resuming from a checkpoint or after migration**
  In rare cases, when a data breakpoint is enabled in the guest OS of virtual machines, during checkpoint resume or after a vSphere vMotion migration, an internal virtualization data structure might be accessed before it is allocated. As a result, the virtual machines crash with core dump and an error such as:
  vcpu-1:VMM fault 14: src=MONITOR rip=0xfffffffffc0XXe00 regs=0xfffffffffcXXXdc0 LBR stack=0xfffffffffcXXXaXX.
  This issue is resolved in this release.

The sfcb daemon might fail with a core dump while installing a third-party CIM provider

The sfcb daemon might try to access already freed memory when registering a CIM provider and fail with a core dump while installing a third-party CIM provider, such as Dell OpenManage Server Administrator for example.

This issue is resolved in this release.

esx-update_7.0.3-0.85.21424296

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A

Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-update_7.0.3-0.85.21424296 • VMware_bootbank_loadesx_7.0.3-0.85.21424296
PRs Fixed	N/A
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

Broadcom-ntg3_4.1.9.0-4vmw.703.0.85.21424296

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_ntg3_4.1.9.0-4vmw.703.0.85.21424296
PRs Fixed	3083426
CVE numbers	N/A

Update the `ntg3` VIB to resolve the following issue:

PR 3083426: You might see jumbo frames packet loss when NICs using the ntg3 driver are connected to certain Dell switches

When NICs using the `ntg3` driver such as Broadcom BCM5719 and BCM5720 are connected to certain models of Dell switches, including but not limited to S4128T-ON and S3048-ON, such NICs might incorrectly drop some of the received packets greater than 6700 bytes. This might cause very low network performance or loss of connectivity.

This issue is resolved in this release. The `ntg3` driver version 4.1.9.0, which is released with ESXi 7.0 Update 3l, contains the fix.

VMware-vmkusb_0.1-8vmw.703.0.85.21424296

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_vmkusb_0.1-8vmw.703.0.85.21424296
PRs Fixed	N/A
CVE numbers	N/A

Updates the `vmkusb` VIB.

VMware-NVMe-PCIe_1.2.3.16-2vmw.703.0.85.21424296

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMW_bootbank_nvme-pcie_1.2.3.16-2vmw.703.0.85.21424296
PRs Fixed	3086841, 3104368, 3061328
CVE numbers	N/A

Update the `nvme-pcie` VIB to resolve the following issues:

PR 3086841: Third-party multipathing plug-ins report "Invalid length RTPG Discriptor" warning while running on the SCSI to NVMe translation stack

In case of an extended header format in the NVMe to SCSI translation layer, third-party multipathing plug-ins such as PowerPath might not account for the extended header size of 4 bytes. As a result, in the `vmkernel.log` , you see an `Invalid length RTPG Descriptor` warning.

This issue is resolved in this release. The fix accounts for 4 bytes of extended headers.

PR 3104368: You cannot install ESXi or create datastores on an NVMe device

When installing ESXi or creating a VMFS datastore on an NVMe device, the native NVMe driver might need to handle a Compare and Write fused operation. According to NVMe specs, the Compare and Write commands must be inserted next to each other in the same Submission Queue, and the Submission Queue Tail doorbell pointer update must indicate both commands as part of one doorbell update. The native NVMe driver puts the two commands together in one Submission Queue, but writes the doorbell for each command separately. As a result, the device firmware might complete the fused commands with an error and fail to create a VMFS datastore. Since creating a VMFS datastore on a device is a prerequisite for successful ESXi installation, you might not be able to install ESXi on such NVMe devices.

This issue is resolved in this release.

PR 3061328: Cannot clear vSAN health check: NVMe device can be identified

If the vSAN health check indicates that an NVMe device cannot be identified, the warning might not be cleared after you correctly select the device model.

This issue is resolved in this release.

ESXi_7.0.3-0.80.21422485

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A

Affected VIBs	• VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.80.21422485 • VMware_bootbank_vdfs_7.0.3-0.80.21422485 • VMware_bootbank_cpu-microcode_7.0.3-0.80.21422485 • VMware_bootbank_crx_7.0.3-0.80.21422485 • VMware_bootbank_esx-xserver_7.0.3-0.80.21422485 • VMware_bootbank_vsanhealth_7.0.3-0.80.21422485 • VMware_bootbank_vsan_7.0.3-0.80.21422485 • VMware_bootbank_esx-ui_2.9.2-21141530 • VMware_bootbank_esxio-combiner_7.0.3-0.80.21422485 • VMware_bootbank_native-misc-drivers_7.0.3-0.80.21422485 • VMware_bootbank_esx-base_7.0.3-0.80.21422485 • VMware_bootbank_gc_7.0.3-0.80.21422485 • VMware_bootbank_bmcal_7.0.3-0.80.21422485 • VMware_bootbank_trx_7.0.3-0.80.21422485
PRs Fixed	N/A
CVE numbers	CVE-2023-1017, CVE-2023-1018

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `esx-dvfilter-generic-fastpath`, `vsan`, `bmcal`, `crx`, `esx-ui`, `esxio-combiner`, `vsanhealth`, `native-misc-drivers`, `gc`, `cpu-microcode`, `vdfs`, `esx-xserver`, `esx-base`, and `trx` VIBs to resolve the following issues:

ESXi 7.0 Update 3l provides the following security updates:

- The Python package is updated to versions 3.8.16/3.5.10.
- The ESXi userworld libxml2 library is updated to version 2.10.3.
- The cURL library is updated to version 7.86.0.
- The Expat XML parser is updated to version 2.5.0.
- The SQLite database is updated to version 3.40.1.
- The zlib library is updated to 1.2.13.

esx-update_7.0.3-0.80.21422485

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_loadesx_7.0.3-0.80.21422485 • VMware_bootbank_esx-update_7.0.3-0.80.21422485
PRs Fixed	N/A
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

VMware-VM-Tools_12.1.5.20735119-21422485

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_locker_tools-light_12.1.5.20735119-21422485
PRs Fixed	3091480
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

- The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3l:
  - **windows.iso**: VMware Tools 12.1.5 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  - **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

  The following VMware Tools ISO images are available for download:
  - VMware Tools 11.0.6:
    - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
  - VMware Tools 10.0.12:
    - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
    - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
  - **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
  - **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. Refer VMware knowledge base article 88698 for details.

  Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:
  - Updating VMware Tools
  - VMware Tools for hosts provisioned with Auto Deploy
  - What Every vSphere Admin Must Know About VMware Tools
  - Earlier versions of VMware Tools
  - VMware Tools 12.1.5 Release Notes

ESXi-7.0U3l-21424296-standard

Profile Name	ESXi-7.0U3l-21424296-standard
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	March 30, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A

Affected VIBs	• VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.85.21424296 • VMware_bootbank_vsan_7.0.3-0.85.21424296 • VMware_bootbank_bmcal_7.0.3-0.85.21424296 • VMware_bootbank_crx_7.0.3-0.85.21424296 • VMware_bootbank_esx-ui_2.9.2-21141530 • VMware_bootbank_esxio-combiner_7.0.3-0.85.21424296 • VMware_bootbank_vsanhealth_7.0.3-0.85.21424296 • VMware_bootbank_native-misc-drivers_7.0.3-0.85.21424296 • VMware_bootbank_gc_7.0.3-0.85.21424296 • VMware_bootbank_cpu-microcode_7.0.3-0.85.21424296 • VMware_bootbank_vdfs_7.0.3-0.85.21424296 • VMware_bootbank_esx-xserver_7.0.3-0.85.21424296 • VMware_bootbank_esx-base_7.0.3-0.85.21424296 • VMware_bootbank_trx_7.0.3-0.85.21424296 • VMware_bootbank_esx-update_7.0.3-0.85.21424296 • VMware_bootbank_loadesx_7.0.3-0.85.21424296 • VMW_bootbank_ntg3_4.1.9.0-4vmw.703.0.85.21424296 • VMW_bootbank_vmkusb_0.1-8vmw.703.0.85.21424296 • VMW_bootbank_nvme-pcie_1.2.3.16-2vmw.703.0.85.21424296 • VMware_locker_tools-light_12.1.5.20735119-21422485
PRs Fixed	3057026, 3062185, 3040049, 3061156, 3023389, 3062861, 3089449, 3081870, 3082900, 3033157, 3090683, 3075786, 3074392, 3081275, 3080022, 3083314, 3084812, 3074360, 3092270, 3076977, 3051685, 3082477, 3082282, 3082427, 3077163, 3087219, 3074187, 3082431, 3050562, 3072430, 3077072, 3077060, 3046875, 3082991, 3083473, 3051059, 3091256, 3074912, 3058993, 3063987, 3072500, 3060661, 3076188, 3049652, 2902475, 3087946, 3116848, 3010502, 3118090, 3078875, 3069298, 3074121, 3083426, 3086841, 3104368, 3061328
Related CVE numbers	CVE-2023-1017, CVE-2023-1018

This patch updates the following issues:

- In the vSphere Client and the ESXi Host Client, you might see incorrect number of sockets and respectively cores per socket when you change the NPS setting on an AMD EPYC 9004 server from the default of 1, or Auto, to another value, such as 2 or 4.
- Due to a rare race condition during a Fast Suspend Resume (FSR) operation on a VM with shared pages between VMs, ESXi hosts might fail with a purple diagnostic screen with an error such as `PFrame_IsBackedByLPage` in the backtrace. The issue occurs during vSphere Storage vMotion operations or hot-adding a device.
- Packet capture with the `-c` option of the `pktcap-uw` utlity in heavy network traffic might be slower than packet capture without the option. You might also see a delay in capturing packets, so that the last package counted has a timestap few seconds earlier than the stop time of the function. The issue results from the `File_GetSize` function to check file sizes, which is slow in VMFS environments and causes low performance of `pktcap-uw` .

- In the `syslog` file you might see frequent log messages such as:
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] *** Received pre-CEE DCBX Packet on port: vmnicX`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info]2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Src MAC: xc:xc:X0:0X:xc:xx`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Dest MAC: X0:xb:xb:fx:0X:X1`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] 2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Port ID TLV:`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] ifName:`
  The issue occurs because the Data Center Bridging (DCB) daemon, `dcbd` , on the ESXi host records unnecessary messages at `/var/log/syslog.log` . As a result, the log file might quickly fill up with `dcbd` logs.
- In some cases, a timed-wait system call in the VMkernel might return too early. As a result, some applications, such as the System Health Agent, might take up to 100% of the CPU usage on one of the ESXi host cores.
- Due to an issue with the IPv6 loopback interfaces, you might not see virtual machine image details in the **Summary** tab of the vSphere Client.
- If the number of paths from an ESXi host using NMP SATP ALUA to storage exceed 255, ESXi ignores part of the ALUA information reported by the target and incorrectly retains some of the path state as active optimised. As a result, some I/Os use the non-optimised path to the storage device and cause latency issues..
- In some cases, during an ESXi host shutdown, helper queues of device probe requests get deleted, but the reference to the device remains. As a result, the ESXi host reboot stops with a message such as `initializing init_VMKernelShutdownHelper: (14/39) ShutdownSCSICleanupForDevTearDown` in the Direct Console User Interface (DCUI).
- Due to a race condition during an Instant Clone operation, VM memory pages might be corrupted and the ESXi host might fail with a purple diagnostic screen. You see errors such as `VmMemMigrate_MarkPagesCow` or `AsyncRemapProcessVMRemapList` in the backtrace.
- In some environments with SATP plug-ins such as `satp_alua` and `satp_alua_cx` , bringing all paths to a LUN online might require several scans. As a result, a storage failover operation might take long. For example, with 4 paths to a LUN, it might take up to 20 minutes to bring the 4 paths online.
- After vSphere vMotion operations across vCenter Server instances for VMs that have vSphere tags, it is possible that the tags do not exist in the target location. The issue only occurs in migration operations between vCenter Server instances that do not share storage.
- When you set the multicast filter mode of an NSX Virtual Switch for NVDS, the mode might intermittently revert from legacy to snooping.
- When you run a Nessus scan, which internally runs a SYN scan, to detect active ports on an ESXi host, the iofiltervpd service might shut down. The service cannot be restarted within the max retry attempts due to the SYN scan.
- If a VIB containing a new kernel module is installed before you run any of the restore config procedures described in VMware knowledge base article 2042141, you see no change in the config after the ESXi host reboots. For example, if you attempt to restore the ESXi config immediately after installing the NSX VIB, the ESXi host reboots, but no changes in the config are visible. The issue occurs due to a logical fault in the updates of the bootbank partition used for ESXi host reboots after a new kernel module VIB is installed.
- Listing files of mounted NFS 4.1 Azure storage might not work as expected, because although the files exist and you can open them by name, the `ls` command on an ESXi host by using SSH does not show any files.
- Starting with ESXi 7.0 Update 1, the `vpxa.cfg` file no longer exists and the vpxa configuration belongs to the ESXi Configuration Store (`ConfigStore`). When you upgrade an ESXi host from a version earlier than 7.0 Update 1 to a later version, the fields `Vpx.Vpxa.config.nfc.loglevel` and `Vpx.Vpxa.config.httpNfc.accessMode` in the `vpxa.cfg` file might cause the ESXi host to fail with a purple diagnostic screen during the conversion from `vpxa.cfg` format to `ConfigStore` format. The issue occurs due to discrepancies in the NFC log level between `vpxa.cfg` and `ConfigStore` , and case-sensitive values.
- In rare cases, multiple concurrent open and close operations on datastores, for example when vSphere DRS triggers multiple migration tasks, might cause some VMs to take longer to complete in-flight disk I/Os. As a result, such virtual

machines might take longer to respond or become unresponsive for a short time. The issue is more likely to occur on VMs that have multiple virtual disks over different datastores.

- During an API call to reload a virtual machine from one ESXi host to another, the `externalId` in the VM port data file might be lost. As a result, after the VM reloads, the VM virtual NIC might not be able to connect to a LSP.
- After upgrading to ESXi 7.0 Update 3i, you might not be able to attach an existing virtual machine disk (VMDK) to a VM by using the VMware Host Client, which is used to connect to and manage single ESXi hosts. The issue does not affect the vSphere Client.
- Due to a race condition between the Create and Delete resource pool workflows, a freed pointer in the VMFS resource pool cache might get dereferenced. As a result, ESXi hosts might fail with a purple diagnostic screen and error such as:
  `@BlueScreen: #PF Exception 14 in world 2105491:res3HelperQu IP 0x420032a21f55 addr 0x0`
- With the batch `QueryUnresolvedVmfsVolume` API, you can query and list unresolved VMFS volumes or LUN snapshots. You can then use other batch APIs to perform operations, such as re-signaturing specific unresolved VMFS volumes. By default, when the API `QueryUnresolvedVmfsVolume` is invoked on a host, the system performs an additional filesystem liveness check for all unresolved volumes that are found. The liveness check detects whether the specified LUN is mounted on other hosts, whether an active VMFS heartbeat is in progress, or if there is any filesystem activity. This operation is time consuming and requires at least 16 seconds per LUN. As a result, when your environment has a large number of snapshot LUNs, the query and listing operation might take significant time.
- This problem can occur when vCenter manages multiple clusters, and the vCenter VM runs on one of the clusters. If you shut down the cluster where the vCenter VM resides, the following error can occur during the shutdown operation: `'NoneType' object has no attribute '_moId'`. The vCenter VM is not powered off.
- This problem can occur when vCenter manages multiple clusters and runs several shut down and restart cluster operations in parallel. For example, if you shut down 3 clusters and restart the vSAN health service or the vCenter VM, and you restart one of the 3 clusters before the others, the **Restart Cluster** option might be available for the first vSAN cluster, but not for the other clusters.
- Unexpected time drift can occur intermittently on a vSAN cluster when a single vCenter Server manages several vSAN clusters, due to internal delays in VPXA requests. In the vSphere Client, in the vSAN Health tab, you see the status of **Time is synchronized across hosts and VC** changing from green to yellow and back to green.
- When you enable the `ToolsRamdisk` advanced option that makes sure the `/vmtools` partition is always on a RAM disk rather than on a USB or SD-card, installing or updating the `tools-light` VIB does not update the content of the RAM disk automatically. Instead, you must reboot the host so that the RAM disk updates and the new VM Tools version is available for the VMs.
- A rare race condition caused by memory reclamation for some performance optimization processes in vSphere vMotion might cause ESXi hosts to fail with a purple diagnostic screen.
- If your environment has both small and large file block clusters mapped to one affinity rule, when you add a cluster, the Affinity Manager might allocate more blocks for files than the actual volume of the datastore. As a result, ESXi hosts randomly fail with a purple diagnostic screen with error `Exception 14 in world #######.`
- This issue occurs when you view health details of any health check in the history view. In the vSphere Client, in the Skyline Health tab, you see a message such as `No data available for the selected time period.` The issue occurs when a query to the historical health records fails due to timestamps with an incorrect time zone.
- The logger command of some logger clients might not pass the right facility code to the ESXi syslog daemon and cause incorrect facility or severity values in ESXi syslog log messages.
- In rare cases, in a heavy workload, two LVM tasks that perform updating and querying on the device schedule in an ESXi host might run in parallel and cause a synchronization issue. As a result, the ESXi host might fail with a purple diagnostic screen and a messages similar to `LVMIoctlInt@com.vmware.lvm.ut#nover+0x1018 stack: 0xXXXXX and Addr3ResolvePhysVector@esx#nover+0x68 stack: 0xXXXX` in the backtrace.
- In some cases, while an ESXi host boots, some dynamically discovered iSCSI targets might get deleted. As a result, after the boot completes, you might no longer see some iSCSI LUNs. The issue is more likely to occur in environments with Challenge-Handshake Authentication Protocol
  (CHAP) enabled for iSCSI.

- In busy environments with many rescans by using a software iSCSI adapter, the VMware Host Client might intermittently stop displaying the adapter. The issue occurs only with target arrays which return target portals with both IPv4 and IPv6 addresses during discovery by using the `SendTargets` method.
- A rare issue with calculating the Max Queue Depth per datastore device might cause queue depth mismatch warnings from the underlying SCSI layer. As a result, when you disable Storage I/O Control on datastores, you might see high read I/O on all ESXi hosts.
- Due to missing configuration for `stats-log` in the file `/etc/vmware/vvold/config.xml`, you might see multiple `-1.log` files to fill up the `/ramdisk` partition after an upgrade to ESXi 7.0 Update 3 and later.
- If a username or password in a network proxy contains any escape character, the environment fails to send network requests through the proxy.
- If you configure an NTP server on an ESXi host with additional parameters along with `hostname`, such as `min_poll` or `max_poll`, the command `esxcli system ntp test` might fail to resolve the IP address of that server. This issue occurs because in such configurations, the NTP name resolution applies to the entire server config instead of just the host name.
- After upgrading to ESXi 7.0 Update 2 and later, a virtual machine might not discover some USB devices attached to it, such as an Eaton USB UPS, and fail to communicate with the device properly.
- If you clone a VM, including the guest customization specs, move the VMDK file to another datastore and make it thick provisioned, and then power on the VM, the guest OS customization might not be preserved. In the hostd logs, you see an Event Type Description such as `The customization component failed to set the required parameters inside the guest operating system.`
  The issue occurs because while moving the VMDK file of the cloned VM to another datastore, the new `pathName` for the guest OS customization might temporarily be the same as the `oldPathName` and the package gets deleted.
- Improper sizing of the resource needs for the hostd service on an ESXi host might cause some virtual machine-related tasks to fail when you use vSphere APIs for I/O Filtering (VAIO) for VMware or third-party backup applications. For example, when a VAIO filter is attached to one or more virtual disks of a virtual machine, such VMs might fail to perform backups or power-on after a backup.
- A rare file corruption issue might occur when multiple ESXi hosts do a simultaneous file append operation on an NFSv3 datastore. As a result, if you use the Govc open source command-line utility to perform administrative actions on a vCenter instance, you might see reports with inconsistent values. For example, if you run the command `govc disk.ls` to list all FCDs in a newly created datastore, you see a different number of disks from what you expect.
- In rare cases, when a VMFS volume is closed immediately after it is opened, one of the threads in the opening process might race with a thread in the closing process and take a rare error handling path that can exit without unlocking a locked spinlock. As a result, the ESXi host might fail with a purple diagnostic screen with a message in the backtrace such as: `@BlueScreen: VERIFY bora/vmkernel/sched/cpusched.c:11154.`
- Due to reservation conflicts, WSFC applications might lose connectivity to a virtual volume-based disk after a rebind operation on that disk.
- In rare situations, the management agent that vSphere HA deploys on ESXi hosts, Fault Domain Manager (FDM), might fail to acquire a vSAN datastore in the first attempt before an exceptional condition, such as power outage, occurs. As a result, vSphere HA failover for virtual machines on that datastore might not be successful. In the vSphere Client, you see a message such as `This virtual machine failed to become vSphere HA Protected and HA may not attempt to restart it after a failure.` Successive attempts of FDM to acquire the vSAN datastore might also fail.
- In the sustainability metrics in VMware vRealize Operations, you might see the value of **Power|Total Energy (Wh)** per virtual machine higher than the ESXi host on which the VM is hosted. The issue occurs because after measuring the total energy consumed by the VM, the **power.energy** performance counter is calculated and reported in millijoules instead of joules.
- In ESXi hosts running on AMD processors, Windows virtual machines of hardware version 19 with VBS enabled might fail with a blue diagnostic screen due to a processor mode misconfiguration error. In the `vmware.log` file, you see errors such as `vcpu-0 - WinBSOD: Synthetic MSR[0xx0000x00] 0xxxx.`
- Due to an internal error, even if a CPU model is listed as supported in the VMware Compatibility Guide, in the vSphere Client you might see a warning such as `The CPU on the host is not supported by the image` during a

compliance scan by using a vSphere Lifecycle Manager image. The warning does not prevent you from completing an update or upgrade.
- When you migrate virtual machines with VBS enabled that reside on ESXi hosts running on AMD processors, such VMs might fail with a blue diagnostic screen on the target host due to a guest interruptibility state error.
- When you override a networking policy such as Teaming, Security, or Shaping for a port group, and then revert the change, after a reboot of the ESXi host, you might still see the override setting. For example, if you accept promiscuous mode activation on a port group level, then revert the mode back to Reject, and reboot the ESXi host, the setting is still Accept.
- Your remote web server might contain an HTML form field that has an input of type `password` and `username` where the `autocomplete` attribute is not set to `off` . As a result, you might see a warning by security scanners such as `AutoComplete Attribute Not Disabled for Password in Form Based Authentication` . The setting of the `autocomplete` attribute to `on` does not directly put a risk on web servers, but in certain browsers, user credentials in such forms might be saved and potentially lead to a loss of confidentiality.
- vSAN Distributed File System (vDFS) objects do not support IOPS limit. You cannot set the IOPS limit for vSAN file service objects.
- In vSphere Client, when you navigate to **Configure** > **Hardware** > **Overview**, for some servers you do not see any asset tag listed.
- When you upgrade a vSAN host from a pre-6.2 release to 7.0 or later, the VMkernel port tagging for vSAN might be lost. If this occurs, vSAN networking configuration is missing after the upgrade.
- You cannot enable vSAN File Service if the vCenter does not have Internet access.
- In rare cases, when a data breakpoint is enabled in the guest OS of virtual machines, during checkpoint resume or after a vSphere vMotion migration, an internal virtualization data structure might be accessed before it is allocated. As a result, the virtual machines crash with core dump and an error such as: vcpu-1:VMM fault 14: src=MONITOR rip=0xffffffffc0XXe00 regs=0xffffffffcXXXdc0 LBR stack=0xffffffffcXXXaXX.
- When NICs using the `ntg3` driver such as Broadcom BCM5719 and BCM5720 are connected to certain models of Dell switches, including but not limited to S4128T-ON and S3048-ON, such NICs might incorrectly drop some of the received packets greater than 6700 bytes. This might cause very low network performance or loss of connectivity.
- In case of an extended header format in the NVMe to SCSI translation layer, third-party multipathing plug-ins such as PowerPath might not account for the extended header size of 4 bytes. As a result, in the `vmkernel.log` , you see an `Invalid length RTPG Descriptor` warning.
- When installing ESXi or creating a VMFS datastore on an NVMe device, the native NVMe driver might need to handle a Compare and Write fused operation. According to NVMe specs, the Compare and Write commands must be inserted next to each other in the same Submission Queue, and the Submission Queue Tail doorbell pointer update must indicate both commands as part of one doorbell update. The native NVMe driver puts the two commands together in one Submission Queue, but writes the doorbell for each command separately. As a result, the device firmware might complete the fused commands with an error and fail to create a VMFS datastore. Since creating a VMFS datastore on a device is a prerequisite for successful ESXi installation, you might not be able to install ESXi on such NVMe devices.
- If the vSAN health check indicates that an NVMe device cannot be identified, the warning might not be cleared after you correctly select the device model.

ESXi-7.0U3l-21424296-no-tools

Profile Name	ESXi-7.0U3l-21424296-no-tools
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	March 30, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A

Affected VIBs	• VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.85.21424296 • VMware_bootbank_vsan_7.0.3-0.85.21424296 • VMware_bootbank_bmcal_7.0.3-0.85.21424296 • VMware_bootbank_crx_7.0.3-0.85.21424296 • VMware_bootbank_esx-ui_2.9.2-21141530 • VMware_bootbank_esxio-combiner_7.0.3-0.85.21424296 • VMware_bootbank_vsanhealth_7.0.3-0.85.21424296 • VMware_bootbank_native-misc-drivers_7.0.3-0.85.21424296 • VMware_bootbank_gc_7.0.3-0.85.21424296 • VMware_bootbank_cpu-microcode_7.0.3-0.85.21424296 • VMware_bootbank_vdfs_7.0.3-0.85.21424296 • VMware_bootbank_esx-xserver_7.0.3-0.85.21424296 • VMware_bootbank_esx-base_7.0.3-0.85.21424296 • VMware_bootbank_trx_7.0.3-0.85.21424296 • VMware_bootbank_esx-update_7.0.3-0.85.21424296 • VMware_bootbank_loadesx_7.0.3-0.85.21424296 • VMW_bootbank_ntg3_4.1.9.0-4vmw.703.0.85.21424296 • VMW_bootbank_vmkusb_0.1-8vmw.703.0.85.21424296 • VMW_bootbank_nvme-pcie_1.2.3.16-2vmw.703.0.85.21424296
PRs Fixed	3057026, 3062185, 3040049, 3061156, 3023389, 3062861, 3089449, 3081870, 3082900, 3033157, 3090683, 3075786, 3074392, 3081275, 3080022, 3083314, 3084812, 3074360, 3092270, 3076977, 3051685, 3082477, 3082282, 3082427, 3077163, 3087219, 3074187, 3082431, 3050562, 3072430, 3077072, 3077060, 3046875, 3082991, 3083473, 3051059, 3091256, 3074912, 3058993, 3063987, 3072500, 3060661, 3076188, 3049652, 2902475, 3087946, 3116848, 3010502, 3118090, 3078875, 3069298, 3074121, 3083426, 3086841, 3104368, 3061328
Related CVE numbers	CVE-2023-1017, CVE-2023-1018

This patch updates the following issues:

- In the vSphere Client and the ESXi Host Client, you might see incorrect number of sockets and respectively cores per socket when you change the NPS setting on an AMD EPYC 9004 server from the default of 1, or Auto, to another value, such as 2 or 4.
- Due to a rare race condition during a Fast Suspend Resume (FSR) operation on a VM with shared pages between VMs, ESXi hosts might fail with a purple diagnostic screen with an error such as `PFrame_IsBackedByLPage` in the backtrace. The issue occurs during vSphere Storage vMotion operations or hot-adding a device.
- Packet capture with the `-c` option of the `pktcap-uw` utlity in heavy network traffic might be slower than packet capture without the option. You might also see a delay in capturing packets, so that the last package counted has a timestap few seconds earlier than the stop time of the function. The issue results from the `File_GetSize` function to check file sizes, which is slow in VMFS environments and causes low performance of `pktcap-uw` .

- In the `syslog` file you might see frequent log messages such as:
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] *** Received pre-CEE DCBX Packet on port: vmnicX`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info]2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Src MAC: xc:xc:X0:0X:xc:xx`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Dest MAC: X0:xb:xb:fx:0X:X1`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] 2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] Port ID TLV:`
  `2022-03-27T00:xx:xx.xxxx dcbd[xxxx]: [info] ifName:`
  The issue occurs because the Data Center Bridging (DCB) daemon, `dcbd` , on the ESXi host records unnecessary messages at `/var/log/syslog.log` . As a result, the log file might quickly fill up with `dcbd` logs.
- In some cases, a timed-wait system call in the VMkernel might return too early. As a result, some applications, such as the System Health Agent, might take up to 100% of the CPU usage on one of the ESXi host cores.
- Due to an issue with the IPv6 loopback interfaces, you might not see virtual machine image details in the **Summary** tab of the vSphere Client.
- If the number of paths from an ESXi host using NMP SATP ALUA to storage exceed 255, ESXi ignores part of the ALUA information reported by the target and incorrectly retains some of the path state as active optimised. As a result, some I/Os use the non-optimised path to the storage device and cause latency issues..
- In some cases, during an ESXi host shutdown, helper queues of device probe requests get deleted, but the reference to the device remains. As a result, the ESXi host reboot stops with a message such as `initializing init_VMKernelShutdownHelper: (14/39) ShutdownSCSICleanupForDevTearDown` in the Direct Console User Interface (DCUI).
- Due to a race condition during an Instant Clone operation, VM memory pages might be corrupted and the ESXi host might fail with a purple diagnostic screen. You see errors such as `VmMemMigrate_MarkPagesCow` or `AsyncRemapProcessVMRemapList` in the backtrace.
- In some environments with SATP plug-ins such as `satp_alua` and `satp_alua_cx` , bringing all paths to a LUN online might require several scans. As a result, a storage failover operation might take long. For example, with 4 paths to a LUN, it might take up to 20 minutes to bring the 4 paths online.
- After vSphere vMotion operations across vCenter Server instances for VMs that have vSphere tags, it is possible that the tags do not exist in the target location. The issue only occurs in migration operations between vCenter Server instances that do not share storage.
- When you set the multicast filter mode of an NSX Virtual Switch for NVDS, the mode might intermittently revert from legacy to snooping.
- When you run a Nessus scan, which internally runs a SYN scan, to detect active ports on an ESXi host, the iofiltervpd service might shut down. The service cannot be restarted within the max retry attempts due to the SYN scan.
- If a VIB containing a new kernel module is installed before you run any of the restore config procedures described in VMware knowledge base article 2042141, you see no change in the config after the ESXi host reboots. For example, if you attempt to restore the ESXi config immediately after installing the NSX VIB, the ESXi host reboots, but no changes in the config are visible. The issue occurs due to a logical fault in the updates of the bootbank partition used for ESXi host reboots after a new kernel module VIB is installed.
- Listing files of mounted NFS 4.1 Azure storage might not work as expected, because although the files exist and you can open them by name, the `ls` command on an ESXi host by using SSH does not show any files.
- Starting with ESXi 7.0 Update 1, the `vpxa.cfg` file no longer exists and the vpxa configuration belongs to the ESXi Configuration Store (`ConfigStore`). When you upgrade an ESXi host from a version earlier than 7.0 Update 1 to a later version, the fields `Vpx.Vpxa.config.nfc.loglevel` and `Vpx.Vpxa.config.httpNfc.accessMode` in the `vpxa.cfg` file might cause the ESXi host to fail with a purple diagnostic screen during the conversion from `vpxa.cfg` format to `ConfigStore` format. The issue occurs due to discrepancies in the NFC log level between `vpxa.cfg` and `ConfigStore` , and case-sensitive values.
- In rare cases, multiple concurrent open and close operations on datastores, for example when vSphere DRS triggers multiple migration tasks, might cause some VMs to take longer to complete in-flight disk I/Os. As a result, such virtual

machines might take longer to respond or become unresponsive for a short time. The issue is more likely to occur on VMs that have multiple virtual disks over different datastores.

- During an API call to reload a virtual machine from one ESXi host to another, the `externalId` in the VM port data file might be lost. As a result, after the VM reloads, the VM virtual NIC might not be able to connect to a LSP.
- After upgrading to ESXi 7.0 Update 3i, you might not be able to attach an existing virtual machine disk (VMDK) to a VM by using the VMware Host Client, which is used to connect to and manage single ESXi hosts. The issue does not affect the vSphere Client.
- Due to a race condition between the Create and Delete resource pool workflows, a freed pointer in the VMFS resource pool cache might get dereferenced. As a result, ESXi hosts might fail with a purple diagnostic screen and error such as:
  `@BlueScreen: #PF Exception 14 in world 2105491:res3HelperQu IP 0x420032a21f55 addr 0x0`
- With the batch `QueryUnresolvedVmfsVolume` API, you can query and list unresolved VMFS volumes or LUN snapshots. You can then use other batch APIs to perform operations, such as re-signaturing specific unresolved VMFS volumes. By default, when the API `QueryUnresolvedVmfsVolume` is invoked on a host, the system performs an additional filesystem liveness check for all unresolved volumes that are found. The liveness check detects whether the specified LUN is mounted on other hosts, whether an active VMFS heartbeat is in progress, or if there is any filesystem activity. This operation is time consuming and requires at least 16 seconds per LUN. As a result, when your environment has a large number of snapshot LUNs, the query and listing operation might take significant time.
- This problem can occur when vCenter manages multiple clusters, and the vCenter VM runs on one of the clusters. If you shut down the cluster where the vCenter VM resides, the following error can occur during the shutdown operation: `'NoneType' object has no attribute '_moId'`. The vCenter VM is not powered off.
- This problem can occur when vCenter manages multiple clusters and runs several shut down and restart cluster operations in parallel. For example, if you shut down 3 clusters and restart the vSAN health service or the vCenter VM, and you restart one of the 3 clusters before the others, the **Restart Cluster** option might be available for the first vSAN cluster, but not for the other clusters.
- Unexpected time drift can occur intermittently on a vSAN cluster when a single vCenter Server manages several vSAN clusters, due to internal delays in VPXA requests. In the vSphere Client, in the vSAN Health tab, you see the status of **Time is synchronized across hosts and VC** changing from green to yellow and back to green.
- When you enable the `ToolsRamdisk` advanced option that makes sure the `/vmtools` partition is always on a RAM disk rather than on a USB or SD-card, installing or updating the `tools-light` VIB does not update the content of the RAM disk automatically. Instead, you must reboot the host so that the RAM disk updates and the new VM Tools version is available for the VMs.
- A rare race condition caused by memory reclamation for some performance optimization processes in vSphere vMotion might cause ESXi hosts to fail with a purple diagnostic screen.
- If your environment has both small and large file block clusters mapped to one affinity rule, when you add a cluster, the Affinity Manager might allocate more blocks for files than the actual volume of the datastore. As a result, ESXi hosts randomly fail with a purple diagnostic screen with error `Exception 14 in world #######.`
- This issue occurs when you view health details of any health check in the history view. In the vSphere Client, in the Skyline Health tab, you see a message such as `No data available for the selected time period.` The issue occurs when a query to the historical health records fails due to timestamps with an incorrect time zone.
- The logger command of some logger clients might not pass the right facility code to the ESXi syslog daemon and cause incorrect facility or severity values in ESXi syslog log messages.
- In rare cases, in a heavy workload, two LVM tasks that perform updating and querying on the device schedule in an ESXi host might run in parallel and cause a synchronization issue. As a result, the ESXi host might fail with a purple diagnostic screen and a messages similar to `LVMIoctlInt@com.vmware.lvm.ut#nover+0x1018 stack: 0xXXXXX and Addr3ResolvePhysVector@esx#nover+0x68 stack: 0xXXXX` in the backtrace.
- In some cases, while an ESXi host boots, some dynamically discovered iSCSI targets might get deleted. As a result, after the boot completes, you might no longer see some iSCSI LUNs. The issue is more likely to occur in environments with Challenge-Handshake Authentication Protocol
  (CHAP) enabled for iSCSI.

- In busy environments with many rescans by using a software iSCSI adapter, the VMware Host Client might intermittently stop displaying the adapter. The issue occurs only with target arrays which return target portals with both IPv4 and IPv6 addresses during discovery by using the `SendTargets` method.
- A rare issue with calculating the Max Queue Depth per datastore device might cause queue depth mismatch warnings from the underlying SCSI layer. As a result, when you disable Storage I/O Control on datastores, you might see high read I/O on all ESXi hosts.
- Due to missing configuration for `stats-log` in the file `/etc/vmware/vvold/config.xml`, you might see multiple `-1.log` files to fill up the `/ramdisk` partition after an upgrade to ESXi 7.0 Update 3 and later.
- If a username or password in a network proxy contains any escape character, the environment fails to send network requests through the proxy.
- If you configure an NTP server on an ESXi host with additional parameters along with `hostname`, such as `min_poll` or `max_poll`, the command `esxcli system ntp test` might fail to resolve the IP address of that server. This issue occurs because in such configurations, the NTP name resolution applies to the entire server config instead of just the host name.
- After upgrading to ESXi 7.0 Update 2 and later, a virtual machine might not discover some USB devices attached to it, such as an Eaton USB UPS, and fail to communicate with the device properly.
- If you clone a VM, including the guest customization specs, move the VMDK file to another datastore and make it thick provisioned, and then power on the VM, the guest OS customization might not be preserved. In the hostd logs, you see an Event Type Description such as `The customization component failed to set the required parameters inside the guest operating system.`
  The issue occurs because while moving the VMDK file of the cloned VM to another datastore, the new `pathName` for the guest OS customization might temporarily be the same as the `oldPathName` and the package gets deleted.
- Improper sizing of the resource needs for the hostd service on an ESXi host might cause some virtual machine-related tasks to fail when you use vSphere APIs for I/O Filtering (VAIO) for VMware or third-party backup applications. For example, when a VAIO filter is attached to one or more virtual disks of a virtual machine, such VMs might fail to perform backups or power-on after a backup.
- A rare file corruption issue might occur when multiple ESXi hosts do a simultaneous file append operation on an NFSv3 datastore. As a result, if you use the Govc open source command-line utility to perform administrative actions on a vCenter instance, you might see reports with inconsistent values. For example, if you run the command `govc disk.ls` to list all FCDs in a newly created datastore, you see a different number of disks from what you expect.
- In rare cases, when a VMFS volume is closed immediately after it is opened, one of the threads in the opening process might race with a thread in the closing process and take a rare error handling path that can exit without unlocking a locked spinlock. As a result, the ESXi host might fail with a purple diagnostic screen with a message in the backtrace such as: `@BlueScreen: VERIFY bora/vmkernel/sched/cpusched.c:11154.`
- Due to reservation conflicts, WSFC applications might lose connectivity to a virtual volume-based disk after a rebind operation on that disk.
- In rare situations, the management agent that vSphere HA deploys on ESXi hosts, Fault Domain Manager (FDM), might fail to acquire a vSAN datastore in the first attempt before an exceptional condition, such as power outage, occurs. As a result, vSphere HA failover for virtual machines on that datastore might not be successful. In the vSphere Client, you see a message such as `This virtual machine failed to become vSphere HA Protected and HA may not attempt to restart it after a failure.` Successive attempts of FDM to acquire the vSAN datastore might also fail.
- In the sustainability metrics in VMware vRealize Operations, you might see the value of **Power|Total Energy (Wh)** per virtual machine higher than the ESXi host on which the VM is hosted. The issue occurs because after measuring the total energy consumed by the VM, the **power.energy** performance counter is calculated and reported in millijoules instead of joules.
- In ESXi hosts running on AMD processors, Windows virtual machines of hardware version 19 with VBS enabled might fail with a blue diagnostic screen due to a processor mode misconfiguration error. In the `vmware.log` file, you see errors such as `vcpu-0 - WinBSOD: Synthetic MSR[0xx0000x00] 0xxxx.`
- Due to an internal error, even if a CPU model is listed as supported in the VMware Compatibility Guide, in the vSphere Client you might see a warning such as `The CPU on the host is not supported by the image` during a

compliance scan by using a vSphere Lifecycle Manager image. The warning does not prevent you from completing an update or upgrade.
- When you migrate virtual machines with VBS enabled that reside on ESXi hosts running on AMD processors, such VMs might fail with a blue diagnostic screen on the target host due to a guest interruptibility state error.
- When you override a networking policy such as Teaming, Security, or Shaping for a port group, and then revert the change, after a reboot of the ESXi host, you might still see the override setting. For example, if you accept promiscuous mode activation on a port group level, then revert the mode back to Reject, and reboot the ESXi host, the setting is still Accept.
- Your remote web server might contain an HTML form field that has an input of type `password` and `username` where the `autocomplete` attribute is not set to `off` . As a result, you might see a warning by security scanners such as `AutoComplete Attribute Not Disabled for Password in Form Based Authentication` . The setting of the `autocomplete` attribute to `on` does not directly put a risk on web servers, but in certain browsers, user credentials in such forms might be saved and potentially lead to a loss of confidentiality.
- vSAN Distributed File System (vDFS) objects do not support IOPS limit. You cannot set the IOPS limit for vSAN file service objects.
- In vSphere Client, when you navigate to **Configure** > **Hardware** > **Overview**, for some servers you do not see any asset tag listed.
- When you upgrade a vSAN host from a pre-6.2 release to 7.0 or later, the VMkernel port tagging for vSAN might be lost. If this occurs, vSAN networking configuration is missing after the upgrade.
- You cannot enable vSAN File Service if the vCenter does not have Internet access.
- In rare cases, when a data breakpoint is enabled in the guest OS of virtual machines, during checkpoint resume or after a vSphere vMotion migration, an internal virtualization data structure might be accessed before it is allocated. As a result, the virtual machines crash with core dump and an error such as: vcpu-1:VMM fault 14: src=MONITOR rip=0xffffffffc0XXe00 regs=0xffffffffcXXXdc0 LBR stack=0xffffffffcXXXaXX.
- When NICs using the `ntg3` driver such as Broadcom BCM5719 and BCM5720 are connected to certain models of Dell switches, including but not limited to S4128T-ON and S3048-ON, such NICs might incorrectly drop some of the received packets greater than 6700 bytes. This might cause very low network performance or loss of connectivity.
- In case of an extended header format in the NVMe to SCSI translation layer, third-party multipathing plug-ins such as PowerPath might not account for the extended header size of 4 bytes. As a result, in the `vmkernel.log` , you see an `Invalid length RTPG Descriptor` warning.
- When installing ESXi or creating a VMFS datastore on an NVMe device, the native NVMe driver might need to handle a Compare and Write fused operation. According to NVMe specs, the Compare and Write commands must be inserted next to each other in the same Submission Queue, and the Submission Queue Tail doorbell pointer update must indicate both commands as part of one doorbell update. The native NVMe driver puts the two commands together in one Submission Queue, but writes the doorbell for each command separately. As a result, the device firmware might complete the fused commands with an error and fail to create a VMFS datastore. Since creating a VMFS datastore on a device is a prerequisite for successful ESXi installation, you might not be able to install ESXi on such NVMe devices.
- If the vSAN health check indicates that an NVMe device cannot be identified, the warning might not be cleared after you correctly select the device model.

ESXi-7.0U3l-21422485-standard

Profile Name	ESXi-7.0U3l-21422485-standard
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	March 30, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A

Affected VIBs	• VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.80.21422485 • VMware_bootbank_vdfs_7.0.3-0.80.21422485 • VMware_bootbank_cpu-microcode_7.0.3-0.80.21422485 • VMware_bootbank_crx_7.0.3-0.80.21422485 • VMware_bootbank_esx-xserver_7.0.3-0.80.21422485 • VMware_bootbank_vsanhealth_7.0.3-0.80.21422485 • VMware_bootbank_vsan_7.0.3-0.80.21422485 • VMware_bootbank_esx-ui_2.9.2-21141530 • VMware_bootbank_esxio-combiner_7.0.3-0.80.21422485 • VMware_bootbank_native-misc-drivers_7.0.3-0.80.21422485 • VMware_bootbank_esx-base_7.0.3-0.80.21422485 • VMware_bootbank_gc_7.0.3-0.80.21422485 • VMware_bootbank_bmcal_7.0.3-0.80.21422485 • VMware_bootbank_trx_7.0.3-0.80.21422485 • VMware_bootbank_loadesx_7.0.3-0.80.21422485 • VMware_bootbank_esx-update_7.0.3-0.80.21422485 • VMware_locker_tools-light_12.1.5.20735119-21422485
PRs Fixed	3091480
Related CVE numbers	CVE-2023-1017, CVE-2023-1018

This patch updates the following issues:

- The Python package is updated to versions 3.8.16/3.5.10.
- The ESXi userworld libxml2 library is updated to version 2.10.3.
- The cURL library is updated to version 7.86.0.
- The Expat XML parser is updated to version 2.5.0.
- The SQLite database is updated to version 3.40.1.
- The zlib library is updated to 1.2.13.

- The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3l:
  - **windows.iso**: VMware Tools 12.1.5 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  - **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

  The following VMware Tools ISO images are available for download:
  - VMware Tools 11.0.6:
    - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
  - VMware Tools 10.0.12:
    - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
    - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
  - **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
  - **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. Refer VMware knowledge base article 88698 for details.

  Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:
  - Updating VMware Tools
  - VMware Tools for hosts provisioned with Auto Deploy
  - What Every vSphere Admin Must Know About VMware Tools
  - Earlier versions of VMware Tools
  - VMware Tools 12.1.5 Release Notes

ESXi-7.0U3l-21422485-no-tools

Profile Name	ESXi-7.0U3l-21422485-no-tools
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	March 30, 2023
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.80.21422485 • VMware_bootbank_vdfs_7.0.3-0.80.21422485 • VMware_bootbank_cpu-microcode_7.0.3-0.80.21422485 • VMware_bootbank_crx_7.0.3-0.80.21422485 • VMware_bootbank_esx-xserver_7.0.3-0.80.21422485 • VMware_bootbank_vsanhealth_7.0.3-0.80.21422485 • VMware_bootbank_vsan_7.0.3-0.80.21422485 • VMware_bootbank_esx-ui_2.9.2-21141530 • VMware_bootbank_esxio-combiner_7.0.3-0.80.21422485 • VMware_bootbank_native-misc-drivers_7.0.3-0.80.21422485 • VMware_bootbank_esx-base_7.0.3-0.80.21422485 • VMware_bootbank_gc_7.0.3-0.80.21422485 • VMware_bootbank_bmcal_7.0.3-0.80.21422485 • VMware_bootbank_trx_7.0.3-0.80.21422485 • VMware_bootbank_loadesx_7.0.3-0.80.21422485

	• VMware_bootbank_esx-update_7.0.3-0.80.21422485
PRs Fixed	3091480
Related CVE numbers	CVE-2023-1017, CVE-2023-1018

This patch updates the following issues:

- The Python package is updated to versions 3.8.16/3.5.10.
- The ESXi userworld libxml2 library is updated to version 2.10.3.
- The cURL library is updated to version 7.86.0.
- The Expat XML parser is updated to version 2.5.0.
- The SQLite database is updated to version 3.40.1.
- The zlib library is updated to 1.2.13.
- The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3l:
  - **windows.iso**: VMware Tools 12.1.5 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  - **linux.iso**: VMware Tools 10.3.25 ISO image for Linux OS with **glibc** 2.11 or later.

  The following VMware Tools ISO images are available for download:
  - VMware Tools 11.0.6:
    - **windows.iso**: for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
  - VMware Tools 10.0.12:
    - **winPreVista.iso**: for Windows 2000, Windows XP, and Windows 2003.
    - **linuxPreGLibc25.iso**: supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with **glibc** version earlier than 2.5.
  - **solaris.iso**: VMware Tools image 10.3.10 for Solaris.
  - **darwin.iso**: Supports Mac OS X versions 10.11 and later. VMware Tools 12.1.0 was the last regular release for macOS. Refer VMware knowledge base article 88698 for details.

  Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:
  - Updating VMware Tools
  - VMware Tools for hosts provisioned with Auto Deploy
  - What Every vSphere Admin Must Know About VMware Tools
  - Earlier versions of VMware Tools
  - VMware Tools 12.1.5 Release Notes

ESXi70U3l-21424296

Name	ESXi
Version	ESXi70U3l-21424296
Release Date	March 30, 2023
Category	Bugfix
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • Broadcom NetXtreme I ESX VMKAPI ethernet driver • Non-Volatile memory controller driver • USB Native Driver for VMware

PRs Fixed	3057026, 3062185, 3040049, 3061156, 3023389, 3062861, 3089449, 3081870, 3082900, 3033157, 3090683, 3075786, 3074392, 3081275, 3080022, 3083314, 3084812, 3074360, 3092270, 3076977, 3051685, 3082477, 3082282, 3082427, 3077163, 3087219, 3074187, 3082431, 3050562, 3072430, 3077072, 3077060, 3046875, 3082991, 3083473, 3051059, 3091256, 3074912, 3058993, 3063987, 3072500, 3060661, 3076188, 3049652, 2902475, 3087946, 3116848, 3010502, 3118090, 3078875, 3069298, 3074121, 3083426, 3086841, 3104368, 3061328
Related CVE numbers	CVE-2023-1017, CVE-2023-1018

ESXi70U3sl-21422485

Name	ESXi
Version	ESXi70U3sl-21422485
Release Date	March 30, 2023
Category	Security
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • ESXi Tools Component
PRs Fixed	3091480
Related CVE numbers	CVE-2023-1017, CVE-2023-1018

Known Issues

Installation, Upgrade and Migration Issues

Corrupted VFAT partitions from a vSphere 6.7 environment might cause upgrades to ESXi 7.x to fail

Due to corrupted VFAT partitions from a vSphere 6.7 environment, repartitioning the boot disks of an ESXi host might fail during an upgrade to ESXi 7.x. As a result, you might see the following errors:When upgrading to ESXi 7.0 Update 3l, the operation fails with a purple diagnostic screen and/or an error such as:

- **An error occurred while backing up VFAT partition files before re-partitioning: Failed to calculate size for temporary Ramdisk: <error>** .
- **An error occurred while backing up VFAT partition files before re-partitioning: Failed to copy files to Ramdisk: <error>** .

  If you use an ISO installer, you see the errors, but no purple diagnostic screen.

When upgrading to an ESXi 7.x version earlier than 7.0 Update 3l, you might see:

- Logs such as **ramdisk (root) is full** in the **vmkwarning.log** file.
- Unexpected rollback to ESXi 6.5 or 6.7 on reboot.
- The **/bootbank**,**/altbootbank**, and ESX-OSData partitions are not present.

Workaround: You must first remediate the corrupted partitions before completing the upgrade to ESXi 7.x. For more details, see VMware knowledge base article 91136.

After upgrading the ntg3 driver to version 4.1.9.0-4vmw, Broadcom NICs with fiber physical connectivity might lose network

Changes in the **ntg3** driver version **4.1.9.0-4vmw** might cause link issues for the fiber physical layer and connectivity on some NICs, such as Broadcom 1Gb, fails to come up.

Workaround: See VMware knowledge base article 92035.

After an upgrade to ESXi 7.0 Update 3l, some ESXi hosts and virtual machines connected to virtual switches might lose network

After an upgrade to ESXi 7.0 Update 3l, some ESXi hosts, their VMs, and other VMkernel ports, such as ports used by vSAN and vSphere Replication, which are connected to virtual switches, might lose connectivity due to an unexpected change in the NIC teaming policy. For example, the teaming policy on a portgroup might change to **Route Based on Originating Virtual Port** from **Route Based on IP Hash**. As a result, such a portgroup might lose network connectivity and some ESXi hosts and their VMs become inaccessible.

Workaround: See VMware knowledge base article 91887.

Known Issues from Previous Releases

The earlier known issues are grouped as follows.

- vSAN Issues
- vSphere Cluster Services Issues
- Installation, Upgrade, and Migration Issues
- Security Features Issues
- Networking Issues
- Storage Issues
- vCenter Server and vSphere Client Issues
- Virtual Machine Management Issues
- vSphere HA and Fault Tolerance Issues
- vSphere Lifecycle Manager Issues
- Miscellaneous Issues
- vSphere Client Issues

vSAN Issues

If you change the preferred site in a VMware vSAN Stretched Cluster, some objects might incorrectly appear as compliant

If you change the preferred site in a stretched cluster, some objects might incorrectly appear as compliant, because their policy settings might not automatically change. For example, if you configure a virtual machine to keep data at the preferred site, when you change the preferred site, data might remain on the nonpreferred site.

Workaround: Before you change a preferred site, in Advanced Settings, lower the `ClomMaxCrawlCycleMinutes` setting to 15 min to make sure objects policies are updated. After the change, revert the `ClomMaxCrawlCycleMinutes` option to the earlier value.

vSphere Cluster Services Issues

You see compatibility issues in new vCLS VMs deployed in vSphere 7.0 Update 3 environment

The default name for new vCLS VMs deployed in vSphere 7.0 Update 3 environment uses the pattern vCLS-UUID. vCLS VMs created in earlier vCenter Server versions continue to use the pattern vCLS (n). Since the use of parenthesis () is not supported by many solutions that interoperate with vSphere, you might see compatibility issues.

Workaround: Reconfigure vCLS by using retreat mode after updating to vSphere 7.0 Update 3.

Installation, Upgrade, and Migration Issues

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Installation of 7.0 Update 1 drivers on ESXi 7.0 hosts might fail

You cannot install drivers applicable to ESXi 7.0 Update 1 on hosts that run ESXi 7.0 or 7.0b.

The operation fails with an error, such as:

```
VMW_bootbank_qedrntv_3.40.4.0-12vmw.701.0.0.xxxxxxx requires vmkapi_2_7_0_0, but the requirement cannot be satisfied within the ImageProfile. Please refer to the log file for more details.
```

Workaround: Update the ESXi host to 7.0 Update 1. Retry the driver installation.

UEFI booting of ESXi hosts might stop with an error during an update to ESXi 7.0 Update 2 from an earlier version of ESXi 7.0

If you attempt to update your environment to 7.0 Update 2 from an earlier version of ESXi 7.0by using vSphere Lifecycle Manager patch baselines, UEFI booting of ESXi hosts might stop with an error such as:

```
Loading /boot.cfgFailed to load crypto64.efiFatal error: 15 (Not found)
```

Workaround: For more information, see VMware knowledge base articles 83063 and 83107 .

If legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract a desired software specification to seed to a new cluster

With vCenter Server 7.0 Update 2, you can create a new cluster by importing the desired software specification from a single reference host. However, if legacy VIBs are in use on an ESXi host, vSphere Lifecycle Manager cannot extract in the vCenter Server instance where you create the cluster a reference software specification from such a host. In the `/var/log/lifecycle.log` , you see messages such as:

```
020-11-11T06:54:03Z lifecycle: 1000082644: HostSeeding:499
ERROR Extract depot failed: Checksum doesn't match. Calculated
5b404e28e83b1387841bb417da93c8c796ef2497c8af0f79583fd54e789d8826, expected:
0947542e30b794c721e21fb595f1851b247711d0619c55489a6a8cae6675e796 2020-11-11T06:54:04Z
lifecycle: 1000082644: imagemanagerctl:366 ERROR Extract depot failed.
2020-11-11T06:54:04Z lifecycle: 1000082644: imagemanagerctl:145 ERROR [VibChecksumError]
```

Workaround: Follow the steps described in VMware knowledge base article 83042.

You see a short burst of log messages in the syslog.log after every ESXi boot

After updating to ESXi 7.0 Update 2, you might see a short burst of log messages after every ESXi boot.

Such logs do not indicate any issue with ESXi and you can ignore these messages. For example:

```
2021-01-19T22:44:22Z watchdog-vaai-nasd: '/usr/lib/vmware/nfs/bin/vaai-nasd -f'
exited after 0 seconds (quick failure 127) 12021-01-19T22:44:22Z watchdog-vaai-
nasd: Executing '/usr/lib/vmware/nfs/bin/vaai-nasd -f'2021-01-19T22:44:22.990Z
aainasd[1000051135]: Log for VAAI-NAS Daemon for NFS version=1.0 build=build-00000
option=DEBUG2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoadFile: No entries
loaded by dictionary.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "/usr/lib/vmware/config": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: DictionaryLoad: Cannot open file "//.vmware/config": No such
file or directory.2021-01-19T22:44:22.990Z vaainasd[1000051135]: DictionaryLoad: Cannot
open file "//.vmware/preferences": No such file or directory.2021-01-19T22:44:22.990Z
vaainasd[1000051135]: Switching to VMware syslog extensions2021-01-19T22:44:22.992Z
vaainasd[1000051135]: Loading VAAI-NAS plugin(s).2021-01-19T22:44:22.992Z
vaainasd[1000051135]: DISKLIB-PLUGIN : Not loading plugin /usr/lib/vmware/nas_plugins/
lib64: Not a shared library.
```

Workaround: None

You see warning messages for missing VIBs in vSphere Quick Boot compatibility check reports

After you upgrade to ESXi 7.0 Update 2, if you check vSphere Quick Boot compatibility of your environment by using the `/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py` command, you might see some warning messages for missing VIBs in the shell. For example:

```
Cannot find VIB(s) ... in the given VIB collection.Ignoring missing reserved VIB(s) ...,
they are removed from reserved VIB IDs.
```

Such warnings do not indicate a compatibility issue.

Workaround: The missing VIB messages can be safely ignored and do not affect the reporting of vSphere Quick Boot compatibility. The final output line of the `loadESXCheckCompat` command unambiguously indicates if the host is compatible.

Auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image fails with an error

If you attempt auto bootstrapping a cluster that you manage with a vSphere Lifecycle Manager image to perform a stateful install and overwrite the VMFS partitions, the operation fails with an error. In the support bundle, you see messages such as:

```
2021-02-11T19:37:43Z Host Profiles[265671 opID=MainThread]: ERROR:
EngineModule::ApplyHostConfig. Exception: [Errno 30] Read-only file system
```

Workaround: Follow vendor guidance to clean the VMFS partition in the target host and retry the operation. Alternatively, use an empty disk. For more information on the disk-partitioning utility on ESXi, see VMware knowledge base article 1036609.

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using ESXCLI might fail due to a space limitation

Upgrades to ESXi 7.x from 6.5.x and 6.7.0 by using the `esxcli software profile update` or `esxcli software profile install` ESXCLI commands might fail, because the ESXi bootbank might be less than the size of the image profile. In the ESXi Shell or the PowerCLI shell, you see an error such as:

```
[InstallationError]
The pending transaction requires 244 MB free space, however the maximum supported size is 239 MB.
```

```
Please refer to the log file for more details.
```

The issue also occurs when you attempt an ESXi host upgrade by using the ESXCLI commands `esxcli software vib update` or `esxcli software vib install`.

Workaround: You can perform the upgrade in two steps, by using the `esxcli software profile update` command to update ESXi hosts to ESXi 6.7 Update 1 or later, and then update to 7.0 Update 1c. Alternatively, you can run an upgrade by using an ISO image and the vSphere Lifecycle Manager.

You cannot migrate linked clones across vCenter Servers

If you migrate a linked clone across vCenter Servers, operations such as power on and delete might fail for the source virtual machine with an `Invalid virtual machine state` error.

Workaround: Keep linked clones on the same vCenter Server as the source VM. Alternatively, promote the linked clone to full clone before migration.

Migration across vCenter Servers of virtual machines with many virtual disks and snapshot levels to a datastore on NVMe over TCP storage might fail

Migration across vCenter Servers of virtual machines with more than 180 virtual disks and 32 snapshot levels to a datastore on NVMe over TCP storage might fail. The ESXi host preemptively fails with an error such as `The migration has exceeded the maximum switchover time of 100 second(s).`

Workaround: None

A virtual machine with enabled Virtual Performance Monitoring Counters (VPMC) might fail to migrate between ESXi hosts

If you try to migrate a virtual machine with enabled VPMC by using vSphere vMotion, the operation might fail if the target host is using some of the counters to compute memory or performance statistics. The operation fails with an error such as `A performance counter used by the guest is not available on the host CPU.`

Workaround: Power off the virtual machine and use cold migration. For more information, see VMware knowledge base article 81191.

If a live VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the upgrade fails

When a VIB install, upgrade, or remove operation immediately precedes an interactive or scripted upgrade to ESXi 7.0 Update 3 by using the installer ISO, the ConfigStore might not keep some configurations of the upgrade. As a result, ESXi hosts become inaccessible after the upgrade operation, although the upgrade seems successful. To prevent this issue, the ESXi 7.0 Update 3 installer adds a temporary check to block such scenarios. In the ESXi installer console, you see the following error message: `Live VIB installation, upgrade or removal may cause subsequent ESXi upgrade to fail when using the ISO installer.`

Workaround: Use an alternative upgrade method to avoid the issue, such as using ESXCLI or the vSphere Lifecycle Manager.

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

The vlanid property in custom installation scripts might not work

If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails

Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

Workaround: None.

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Disable TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or disable automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Security Features Issues

Turn off the Service Location Protocol service in ESXi, slpd, to prevent potential security vulnerabilities

Some services in ESXi that run on top of the host operating system, including slpd, the CIM object broker, sfcbd, and the related openwsmand service, have proven security vulnerabilities. VMware has addressed all known vulnerabilities in VMSA-2019-0022 and VMSA-2020-0023, and the fixes are part of the vSphere 7.0 Update 2 release. While sfcbd and openwsmand are disabled by default in ESXi, slpd is enabled by default and you must turn it off, if not necessary, to prevent exposure to a future vulnerability after an upgrade.

Workaround: To turn off the slpd service, run the following PowerCLI commands:

```
$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Set-VMHostService -policy "off"$ Get-VMHost | Get-VmHostService | Where-Object {$_.key -eq "slpd"} | Stop-VMHostService -Confirm:$false
```

Alternatively, you can use the command `chkconfig slpd off && /etc/init.d/slpd stop`.

The openwsmand service is not on the ESXi services list and you can check the service state by using the following PowerCLI commands:

```
$esx=(Get-EsxCli -vmhost xx.xx.xx.xx -v2)$esx.system.process.list.invoke() | where CommandLine -like '*openwsman*' | select commandline
```

In the ESXi services list, the sfcbd service appears as sfcbd-watchdog.

For more information, see VMware knowledge base articles 76372 and 1025757.

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can disable the queue-pair with a module parameter. To disable the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

One or more I/O devices do not generate interrupts when the AMD IOMMU is in use

If the I/O devices on your ESXi host provide more than a total of 512 distinct interrupt sources, some sources are erroneously assigned an interrupt-remapping table entry (IRTE) index in the AMD IOMMU that is greater than the maximum value. Interrupts from such a source are lost, so the corresponding I/O device behaves as if interrupts are disabled.

Workaround: Use the ESXCLI command `esxcli system settings kernel set -s iovDisableIR -v true` to disable the AMD IOMMU interrupt remapper. Reboot the ESXi host so that the command takes effect.

When you set auto-negotiation on a network adapter, the device might fail

In some environments, if you set link speed to auto-negotiation for network adapters by using the command `esxcli network nic set -a -n vmmicx`, the devices might fail and reboot does not recover connectivity. The issue is specific to a combination of some Intel X710/X722 network adapters, a SFP+ module and a physical switch, where auto-negotiate speed/duplex scenario is not supported.

Workaround: Make sure you use an Intel-branded SFP+ module. Alternatively, use a Direct Attach Copper (DAC) cable.

Solarflare x2542 and x2541 network adapters configured in 1x100G port mode achieve throughput of up to 70Gbps in a vSphere environment

vSphere 7.0 Update 2 supports Solarflare x2542 and x2541 network adapters configured in 1x100G port mode. However, you might see a hardware limitation in the devices that causes the actual throughput to be up to some 70Gbps in a vSphere environment.

Workaround: None

VLAN traffic might fail after a NIC reset

A NIC with PCI device ID 8086:1537 might stop to send and receive VLAN tagged packets after a reset, for example, with a command `vsish -e set /net/pNics/vmnic0/reset 1`.

Workaround: Avoid resetting the NIC. If you already face the issue, use the following commands to restore the VLAN capability, for example at vmnic0:

```
# esxcli network nic software set --tagging=1 -n vmnic0# esxcli network nic software set --tagging=0 -n vmnic0
```

Any change in the NetQueue balancer settings causes NetQueue to be disabled after an ESXi host reboot

Any change in the NetQueue balancer settings by using the command `esxcli/localcli network nic queue loadbalancer set -n <nicname> --<lb_setting>` causes NetQueue, which is enabled by default, to be disabled after an ESXi host reboot.

Workaround: After a change in the NetQueue balancer settings and host reboot, use the command `configstorecli config current get -c esx -g network -k nics` to retrieve ConfigStore data to verify whether the `/esx/network/nics/net_queue/load_balancer/enable` is working as expected.

After you run the command, you see output similar to:

```
{"mac": "02:00:0e:6d:14:3e","name": "vmnic1","net_queue": { "load_balancer":
{ "dynamic_pool": true, "enable": true }},"virtual_mac": "00:50:56:5a:21:11"}
```

If the output is not as expected, for example `"load_balancer": "enable": false"` , run the following command:

```
esxcli/localcli network nic queue loadbalancer state set -n <nicname> -e true
```

Paravirtual RDMA (PVRDMA) network adapters do not support NSX networking policies

If you configure an NSX distributed virtual port for use in PVRDMA traffic, the RDMA protocol traffic over the PVRDMA network adapters does not comply with the NSX network policies.

Workaround: Do not configure NSX distributed virtual ports for use in PVRDMA traffic.

Rollback from converged vSphere Distributed Switch (VDS) to NSX-T VDS is not supported in vSphere 7.0 Update 3

Rollback from converged VDS that supports both vSphere 7 traffic and NSX-T 3 traffic on the same VDS to one N-VDS for NSX-T traffic is not supported in vSphere 7.0 Update 3.

Workaround: None

If you do not set the nmlx5 network driver module parameter, network connectivity or ESXi hosts might fail

If you do not set the `supported_num_ports` module parameter for the `nmlx5_core` driver on an ESXi host with multiple network adapters of versions Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6, the driver might not allocate sufficient memory for operating all the NIC ports for the host. As a result, you might experience network loss or ESXi host failure with purple diagnostic screen, or both.

Workaround: Set the `supported_num_ports` module parameter value in the `nmlx5_core` network driver equal to the total number of Mellanox ConnectX-4, Mellanox ConnectX-5 and Mellanox ConnectX-6 network adapter ports on the ESXi host.

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

vCenter Server fails if the hosts in a cluster using Distributed Resource Scheduler (DRS) join NSX-T networking by a different Virtual Distributed Switch (VDS) or combination of NSX-T Virtual Distributed Switch (NVDS) and VDS

In vSphere 7.0, when using NSX-T networking on vSphere VDS with a DRS cluster, if the hosts do not join the NSX transport zone by the same VDS or NVDS, it can cause vCenter Server to fail.

Workaround: Have hosts in a DRS cluster join the NSX transport zone using the same VDS or NVDS.

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

A VMFS datastore backed by an NVMe over Fabrics namespace or device might become permanently inaccessible after recovering from an APD or PDL failure

If a VMFS datastore on an ESXi host is backed by an NVMe over Fabrics namespace or device, in case of an all paths down (APD) or permanent device loss (PDL) failure, the datastore might be inaccessible even after recovery. You cannot access the datastore from either the ESXi host or the vCenter Server system.

Workaround: To recover from this state, perform a rescan on a host or cluster level. For more information, see Perform Storage Rescan.

Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

Attempts to attach multiple CNS volumes to the same pod might occasionally fail with an error

When you attach multiple volumes to the same pod simultaneously, the attach operation might occasionally choose the same controller slot. As a result, only one of the operations succeeds, while other volume mounts fail.

Workaround: After Kubernetes retries the failed operation, the operation succeeds if a controller slot is available on the node VM.

Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Linked Software-Defined Data Center (SDDC) vCenter Server instances appear in the on-premises vSphere Client if a vCenter Cloud Gateway is linked to the SDDC.

When a vCenter Cloud Gateway is deployed in the same environment as an on-premises vCenter Server, and linked to an SDDC, the SDDC vCenter Server will appear in the on-premises vSphere Client. This is unexpected behavior and the linked SDDC vCenter Server should be ignored. All operations involving the linked SDDC vCenter Server should be performed on the vSphere Client running within the vCenter Cloud Gateway.

Workaround: None.

Virtual Machine Management Issues

UEFI HTTP booting of virtual machines on ESXi hosts of version earlier than 7.0 Update 2 fails

UEFI HTTP booting of virtual machines is supported only on hosts of version ESXi 7.0 Update 2 and later and VMs with HW version 19 or later.

Workaround: Use UEFI HTTP booting only in virtual machines with HW version 19 or later. Using HW version 19 ensures the virtual machines are placed only on hosts with ESXi version 7.0 Update 2 or later.

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10

Virtual machine snapshot operations fail in vSphere Virtual Volumes datastores on Purity version 5.3.10 with an error such as `An error occurred while saving the snapshot: The VVol target encountered a vendor specific error.` The issue is specific for Purity version 5.3.10.

Workaround: Upgrade to Purity version 6.1.7 or follow vendor recommendations.

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Disable Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first disable vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be disabled on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, adding hosts causes a vSphere HA error state

Adding one or multiple ESXi hosts during a remediation process of a vSphere HA enabled cluster, results in the following error message: `Applying HA VIBs on the cluster encountered a failure.`

Workaround: After the cluster remediation operation has finished, perform one of the following tasks.

- Right-click the failed ESXi host and select *Reconfigure for vSphere HA*.
- Disable and re-enable vSphere HA for the cluster.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, disable and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

Importing an image with no vendor addon, components, or firmware and drivers addon to a cluster which image contains such elements, does not remove the image elements of the existing image

Only the ESXi base image is replaced with the one from the imported image.

Workaround: After the import process finishes, edit the image, and if needed, remove the vendor addon, components, and firmware and drivers addon.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can disable DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

If you run the ESXCLI command to unload the firewall module, the hostd service fails and ESXi hosts lose connectivity

If you automate the firewall configuration in an environment that includes multiple ESXi hosts, and run the ESXCLI command `esxcli network firewall unload` that destroys filters and unloads the firewall module, the hostd service fails and ESXi hosts lose connectivity.

Workaround: Unloading the firewall module is not recommended at any time. If you must unload the firewall module, use the following steps:

1. Stop the hostd service by using the command: `/etc/init.d/hostd stop.`
2. Unload the firewall module by using the command: `esxcli network firewall unload.`
3. Perform the required operations.
4. Load the firewall module by using the command: `esxcli network firewall load.`
5. Start the hostd service by using the command: `/etc/init.d/hostd start.`

vSphere Storage vMotion operations might fail in a vSAN environment due to an unauthenticated session of the Network File Copy (NFC) manager

Migrations to a vSAN datastore by using vSphere Storage vMotion of virtual machines that have at least one snapshot and more than one virtual disk with different storage policy might fail. The issue occurs due to an unauthenticated session of the NFC manager because the Simple Object Access Protocol (SOAP) body exceeds the allowed size.

Workaround: First migrate the VM home namespace and just one of the virtual disks. After the operation completes, perform a disk only migration of the remaining 2 disks.

Changes in the properties and attributes of the devices and storage on an ESXi host might not persist after a reboot

If the device discovery routine during a reboot of an ESXi host times out, the jumpstart plug-in might not receive all configuration changes of the devices and storage from all the registered devices on the host. As a result, the process might restore the properties of some devices or storage to the default values after the reboot.

Workaround: Manually restore the changes in the properties of the affected device or storage.

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations

If you use a beta build of ESXi 7.0, ESXi hosts might fail with a purple diagnostic screen during some lifecycle operations such as unloading a driver or switching between ENS mode and native driver mode. For example, if you try to change the ENS mode, in the backtrace you see an error message similar to: `case ENS::INTERRUPT::NoVM_DeviceStateWithGracefulRemove hit BlueScreen: ASSERT bora/vmkernel/main/dlmalloc.c:2733` This issue is specific for beta builds and does not affect release builds such as ESXi 7.0.

Workaround: Update to ESXi 7.0 GA.

You cannot create snapshots of virtual machines due to an error that a digest operation has failed

A rare race condition when an All-Paths-Down (APD) state occurs during the update of the Content Based Read Cache (CBRC) digest file might cause inconsistencies in the digest file. As a result, you cannot create virtual machine snapshots. You see an error such as `An error occurred while saving the snapshot: A digest operation has failed` in the backtrace.

Workaround: Power cycle the virtual machines to trigger a recompute of the CBRC hashes and clear the inconsistencies in the digest file.

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, Trusted Platform Module (TPM) attestation of the ESXi hosts fails

If you upgrade your ESXi hosts to version 7.0 Update 3, but your vCenter Server is of an earlier version, and you enable TPM, ESXi hosts fail to pass attestation. In the vSphere Client, you see the warning Host TPM attestation alarm. The Elliptic Curve Digital Signature Algorithm (ECDSA) introduced with ESXi 7.0 Update 3 causes the issue when vCenter Server is not of version 7.0 Update 3.

Workaround: Upgrade your vCenter Server to 7.0 Update 3 or acknowledge the alarm.

You see warnings in the boot loader screen about TPM asset tags

If a TPM-enabled ESXi host has no asset tag set on, you might see idle warning messages in the boot loader screen such as:

```
Failed to determine TPM asset tag size: Buffer too smallFailed to measure asset tag into TPM: Buffer too small
```

Workaround: Ignore the warnings or set an asset tag by using the command `$ esxcli hardware tpm tag set -d`

The sensord daemon fails to report ESXi host hardware status

A logic error in the IPMI SDR validation might cause `sensord` to fail to identify a source for power supply information. As a result, when you run the command `vsish -e get /power/hostStats` , you might not see any output.

Workaround: None

If an ESXi host fails with a purple diagnostic screen, the netdump service might stop working

In rare cases, if an ESXi host fails with a purple diagnostic screen, the netdump service might fail with an error such as `NetDump FAILED: Couldn't attach to dump server at IP x.x.x.x.`

Workaround: Configure the VMkernel core dump to use local storage.

You see frequent VMware Fault Domain Manager (FDM) core dumps on multiple ESXi hosts

In some environments, the number of datastores might exceed the FDM file descriptor limit. As a result, you see frequent core dumps on multiple ESXi hosts indicating FDM failure.

Workaround: Increase the FDM file descriptor limit to 2048. You can use the setting `das.config.fdm.maxFds` from the vSphere HA advanced options in the vSphere Client. For more information, see Set Advanced Options.

Virtual machines on a vSAN cluster with enabled NSX-T and a converged vSphere Distributed Switch (CVDS) in a VLAN transport zone cannot power on after a power off

If a secondary site is 95% disk full and VMs are powered off before simulating a secondary site failure, during recovery some of the virtual machines fail to power on. As a result, virtual machines become unresponsive. The issue occurs regardless if site recovery includes adding disks or ESXi hosts or CPU capacity.

Workaround: Select the virtual machines that do not power on and change the network to VM Network from Edit Settings on the VM context menu.

ESXI hosts might fail with a purple diagnostic screen with an error Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835

In rare cases, for example when running SESparse tests, the number of locks per transaction in a VMFS datastore might exceed the limit of 50 for the `J6_MAX_TXN_LOCKACTIONS` parameter. As a result, ESXi hosts might fail with a purple diagnostic screen with an error `Assert at bora/modules/vmkernel/vmfs/fs6Journal.c:835` .

Workaround: None

If you modify the netq_rss_ens parameter of the nmlx5_core driver, ESXi hosts might fail with a purple diagnostic screen

If you try to enable the `netq_rss_ens` parameter when you configure an enhanced data path on the `nmlx5_core` driver, ESXi hosts might fail with a purple diagnostic screen. The `netq_rss_ens` parameter, which enables NetQ RSS, is disabled by default with a value of `0` .

Workaround: Keep the default value for the `netq_rss_ens` module parameter in the `nmlx5_core` driver.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Disable the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

Upgrade to ESXi 7.0 Update 3 might fail due to changed name of the inbox i40enu network driver

Starting with vSphere 7.0 Update 3, the inbox i40enu network driver for ESXi changes name back to i40en. The i40en driver was renamed to i40enu in vSphere 7.0 Update 2, but the name change impacted some upgrade paths. For example, rollup upgrade of ESXi hosts that you manage with baselines and baseline groups from 7.0 Update 2 or 7.0 Update 2a to 7.0 Update 3 fails. In most cases, the i40enu driver upgrades to ESXi 7.0 Update 3 without any additional steps. However, if the driver upgrade fails, you cannot update ESXi hosts that you manage with baselines and baseline groups. You also cannot use host seeding or a vSphere Lifecycle Manager single image to manage the ESXi hosts. If you have already made changes related to the i40enu driver and devices in your system, before upgrading to ESXi 7.0 Update 3, you must uninstall the i40enu VIB or Component on ESXi, or first upgrade ESXi to ESXi 7.0 Update 2c.

Workaround: For more information, see VMware knowledge base article 85982.

SSH access fails after you upgrade to ESXi 7.0 Update 3d

After you upgrade to ESXi 7.0 Update 3d, SSH access might fail in certain conditions due to an update of OpenSSH to version 8.8.

Workaround: For more information, see VMware knowledge base article 88055.

USB device passthrough from ESXi hosts to virtual machines might fail

A USB modem device might simultaneously claim multiple interfaces by the VMkernel and block the device passthrough to VMs.

Workaround: You must apply the USB.quirks advanced configuration on the ESXi host to ignore the NET interface from VMkernel and allow the USB modem to passthrough to VMs. You can apply the configuration in 3 alternative ways:

1. Access the ESXi shell and run the following command: `esxcli system settings advanced set -o /USB/quirks -s 0xvvvv:0xpppp:0:0xffff:UQ_NET_IGNORE | |- Device Product ID |------- Device Vendor ID`
   For example, for the Gemalto M2M GmbH Zoom 4625 Modem(`vid:pid/1e2d:005b`), you can have the command `esxcli system settings advanced set` **-o** `/USB/quirks -s 0x1e2d:0x005b:0:0xffff:UQ_NET_IGNORE`
   Reboot the ESXi host.
2. Set the advanced configuration from the vSphere Client or the vSphere Web Client and reboot the ESXi host.
3. Use a Host Profile to apply the advanced configuration.

For more information on the steps, see VMware knowledge base article 80416.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

vSphere Client Issues

BIOS manufacturer displays as "--" in the vSphere Client

In the vSphere Client, when you select an ESXi host and navigate to **Configure** > **Hardware** > **Firmware**, you see `--` instead of the BIOS manufacturer name.

Workaround: For more information, see VMware knowledge base article 88937.

ESXi Release Notes Before Mar'23

Release notes published before March 2023 are available in pdf format:

VMware vSphere

VMware vSphere 7.0 Release Notes

VMware ESXi

VMware ESXi 7.0 Update 3k Release Notes

VMware ESXi 7.0 Update 3j Release Notes
VMware ESXi 7.0 Update 3i Release Notes
VMware ESXi 7.0 Update 3g Release Notes
VMware ESXi 7.0 Update 3f Release Notes
VMware ESXi 7.0 Update 3e Release Notes
VMware ESXi 7.0 Update 3d Release Notes
VMware ESXi 7.0 Update 2e Release Notes
VMware ESXi 7.0 Update 1e Release Notes
VMware ESXi 7.0 Update 3c Release Notes
VMware ESXi 7.0 Update 2d Release Notes
VMware ESXi 7.0 Update 2c Release Notes
VMware ESXi 7.0 Update 2a Release Notes
VMware ESXi 7.0 Update 2 Release Notes
VMware ESXi 7.0 Update 1d Release Notes
VMware ESXi 7.0 Update 1c Release Notes
VMware ESXi 7.0 Update 1b Release Notes
VMware ESXi 7.0 Update 1a Release Notes
VMware ESXi 7.0 Update 1 Release Notes
VMware ESXi 7.0, Patch Release ESXi 7.0b

vCenter Server Update and Patch Release Notes

VMware vCenter Server 7.0 Update 3u Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3u | 31 MAR 2025 | ISO Build 24614210 Check for additions and updates to these release notes.

What's New

- VMware vCenter Server 7.0 Update 3u serves as a vehicle for VMware vSphere with Tanzu and does not deliver vCenter Server fixes.

Patches Contained in This Release

Patch for VMware vCenter 7.0 Update 3u

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02300-24614210-patch-FP.iso
Build	24614210
Download Size	6701.3 MB
md5sum	3ca90d9abb05a79c1b76ff0c573b0228
sha256checksum	483ec3c8184281e69f720ff11d0ad896fc709b1785ec20409f12360f9a83a629
PRs fixed	3479424
CVEs	N/A

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      ```
      kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify
      ```
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      ```
      kubectl config use-context <namespace_name>
      ```
      and
      ```
      kubectl describe pod <pod_name> -n <namespace_name>
      ```

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10
```

```
IPs:
IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

`RuntimeError: unidentifiable C++ exception.`

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the`/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.

3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error.`

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.

2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR).

Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the

setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3v Release Notes

This document contains the following sections

- Introduction
- What's New
- Upgrade Notes
- Patches Contained in This Release
- Resolved Issues
- Known Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3v | 20 MAY 2025 | ISO Build 24730281 Check for additions and updates to these release notes.

What's New

- For vCenter Server 7.0 Update 3v updates, see the **Resolved Issues** and **Known Issues** sections.
- For vSphere Supervisor updates, see the vSphere Supervisor Release Notes.
- For Photon OS updates, see VMware vCenter Server Appliance Photon OS Security Patches.

This release resolves CVE-2025-41225. For more information on this vulnerability and its impact on Broadcom products, see VMSA-2025-0010.

Prefix-Based MAC Address Allocation by the vCenter GUI Installer and CLI:

vCenter 7.0 Update 3v adds the option to use prefix-based allocation to specify an OUI other than the default one 00:50:56 by Broadcom, or to introduce Locally Administered MAC Addresses (LAA) for a larger address space, by using either the vCenter GUI installer or the CLI installer. After deploying a vCenter instance, you can use the vSphere Client to switch between the available allocation schemes.

Upgrade Notes

Upgrading from vCenter 7.0 Update 3v to vCenter 8.0 Update 3e is not supported due to back-in-time release restrictions. For more information, see KB 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3v

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02400-24730281-patch-FP.iso
Build	24730281
Download Size	6686.0 MB
md5sum	33bb110f457ec1d06054cb4362476c22
sha256checksum	00d688b44ff746e59ba9c5cf60d4c6dc791ba70814f46102795f506717973ef4
PRs fixed	3404100, 3404108, 3471234, 3503319, 3484455, 3484244, 3245536, 3426087, 3473337, 3407726, 3384385, 3418166, 3367090, 3444766, 3468763, 3486798, 3419045
CVEs	CVE-2025-41225

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

vCenter and vSphere Client Issues

PR 3404100: vCenter performance stats shows incorrect aggregate values when the data is rolled up to the daily partition

Without date rounding logic, the partition index might start at a random hour instead of 00:00:00, leading to incorrect aggregate values when the data is rolled up to the daily partition.

This issue is resolved in this release.

PR 3404108: Rollup processing of performance stats data in vCenter occurs only by the average rollup type

In vCenter performance statistics, you see only the average value of each duration, regardless if the rollup type is different, such as summation or latest.

This issue is resolved in this release.

PR 3471234: Smart card authentication on vCenter intermittently fails with the error "Unable to validate submitted credentials"

The Certificate Revocation List (CRL) cache updates hourly and if you log in to vCenter by using a smart card during such an hourly cycle in which the old CRL is expired but no new CRL is downloaded, the login fails. Since this is a corner

case, smart card authentication on vCenter intermittently fails and in the vSphere Client, you see the error `Unable to validate submitted credentials.`

This issue is resolved in this issue.

PR 3503319: The vpxd service fails because the Guest OS customization API requires IPv4 settings

When you use API to create a Guest Customization Specification and customize the guest OS of a virtual machine, you might need to enter IPv4 settings in the specification or the vpxd service fails with a core dump.

This issue is resolved in this release.

PR 3484455: Distributed Resource Scheduler (DRS) fails to migrate an encrypted VM with an error for missing [Cryptographic operations > Migrate] privileges

In some cases, when DRS schedules to migrate an encrypted VM, it might use the context of a user without `Cryptographer.Migrate` privilege and migration fails with an error in the vSphere Client such as: `Permission to perform this operation was denied. You do not hold privileges "virtual machine vm-xx : [Cryptographic operations > Migrate].`

In the vpxd.log, you see error messages such as:

`YYYY-MM-DDThh:mm:ss.472Z info vpxd[06061] [Originator@6876 sub=drsExec opID=<op_id>] Executing DRM recommended vMotion in [vim.ClusterComputeResource:domain-c<id>,esxi_name], migrating [vim.VirtualMachine:vm-<vm_id>,vm_name] from vim.HostSystem:host-<src_id> to vim.HostSystem:host-<dstn_id>……..`

`YYYY-MM-DDThh:mm:ss.494Z info vpxd[06061] [Originator@6876 sub=pbm opID=<op_id>-01] pre migrate callback is skipped - for cached from pre migrate check reason`

`YYYY-MM-DDThh:mm:ss.494Z warning vpxd[06061] [Originator@6876 sub=CryptoManager opID=<op_id>-01] The session xx-yy-zz of user DOMAIN\user_name does not have privilege Cryptographer.Migrate on entity [vim.VirtualMachine:vm-<vm_id>,vm_name].`

This issue is resolved in this release.

PR 3484244: A rare race condition might cause repeating failovers due to a failure of the vCenter vpxd service or the vSphere Client becoming unresponsive

A rare race condition during a VAPI call from the vpxd service to a virtual machine that coincides with the deletion of a `VirtualMachine` object might cause the vpxd service to fail. As a result, you see repeating failovers or the vSphere Client might become unresponsive.

This issue is resolved in this release.

PR 3245536: When an ESXi host has multiple management IP addresses, in some vSphere Client workflows you might see a "Host not reachable" error

You can assign multiple management IP addresses to a single ESXi host and it is not necessary that all IP addresses are reachable from vCenter at any time. However, if vCenter picks a currently unreachable IP during a workflow that you run from the vSphere Client, such as a remediation precheck, the task might fail with a `Host not reachable` error.

This issue is resolved in this release.

Networking Issues

PR 3351967: Stale NSX properties from ESXi hosts that vCenter might use can cause various networking issues

In some cases, vCenter might retrieve NSX properties from ESXi hosts, save them on the vCenter database and push these NSX properties back to ESXi hosts in various scenarios that can cause the following issues:

1. A virtual switch gets out of sync because vCenter pushes stale NSX properties to an ESXi host.

2. You cannot remove the NSX VIB after you remove a transport node, because vCenter pushes NSX properties back to the virtual switch.
3. After an ESXi host reboot, vCenter feeds stale NSX properties back to the virtual switch.
4. NSX cannot start on a virtual switch due to stale NSX properties.

Logs are different in each case, but you can confirm the issue by checking the `VPX_DVS_BLOB` table in the vCenter DB. If you see NSX properties in the `VPX_DVS_BLOB` table, the issue exists. Look for properties such as:

```
com.vmware.nsx.kcp.enable

com.vmware.nsx.spf.enabled

com.vmware.nsx.vdl2.enabled

com.vmware.vswitch.disabled

com.vmware.host.feature.container

com.vmware.nsx.ens.loadbal

com.vmware.nsx.ens.overlayl2flow
```

This issue is resolved in this release.

PR 3426087: You see duplicate routes in the Netplan configuration file after guest OS customization on Ubuntu VMs

For Ubuntu releases that support the Netplan utility for configuring networking on a Linux system, when you deploy an Ubuntu VM and customize it with both IPv4 and IPv6 gateways, the Netplan configuration file `/etc/netplan/99-netcfg-vmware.yaml` of the guest OS contains two route sections under a single network interface.

This issue is resolved in this release. With the fix, customizing an Ubuntu VM with both IPv4 and IPv6 gateways creates a single route section for each NIC in the Netplan configuration file, and adds the corresponding IPv4 and IPv6 gateways of the NIC to its route section.

PR 3473337: In the vSphere Client, you still see an NSX overlay segment after deleting it from the NSX Manager

When adding NSX port groups on a vCenter system, vCenter uses an API call to push the port groups to ESXi hosts, but in some cases the call does not complete on all hosts, if a host is temporarily disconnected for example. As a result, from vCenter perspective, all port groups exist, but from ESXi hosts perspective, some might not exist. Consequently, when you try to delete an NSX overlay segment from the NSX Manager, it still shows in the vSphere Client, because not all port groups can be removed.

This issue is resolved in this release.

PR 3407726: If the Key Management Server (KMS) sends a response not in Key Management Interoperability Protocol (KMIP) format, the vpxd service might fail

In rare cases, KMS might send a response that does not follow the KMIP protocol, which leads to the use of an invalid address in analyzing the response and in turn causes the vpxd service to fail.

This issue is resolved in this release.

PR 3384385: The vpxd service fails after the Mobility Agent (MA) host for VMware HCX is reconnected or redeployed

When you reconnect or redeploy the MA service, which is the data proxy for vSphere vMotion in HCX between onprem and cloud migrations, as a host object in vCenter, the vpxd service might fail due to duplicate entries in the vCenter database. In the vpxd log, you see messages such as `ODBC error: (23505) - ERROR: duplicate key value violates unique constraint "pk_vpx_nw_assignment.`

This issue is resolved in this release.

PR 3418166: You don't see newly created NSX Distributed Virtual port groups on some ESXi hosts

When multiple ESXi hosts join a new transport zone, a race condition in the vCenter host sync handler might cause some ESXi hosts to fail saving the new transport zones configuration. As a result, you don't see newly created NSX Distributed Virtual port groups in the new transport zone on such hosts.

This issue is resolved in this release.

Miscellaneous Issues

PR 3367090: Changes in the authorization roles on an ESXi host are not persistent across reboots

Due to an issue with saving changes to the underlying storage, modifications of the authorization roles on an ESXi host, such as adding a privilege, might not persist across reboots.

This issue is resolved in this release.

PR 3444766: vCenter CPU utilization reaches 100% and the vCenter system becomes slow or unresponsive

After several days of uptime, due to an issue with the Apache HttpCore library, the vCenter CPU utilization by the `vsphere-ui` service might reach 100% and the vCenter system becomes slow or unresponsive.

This issue is resolved in this release.

Upgrade Issues

PR 3468763: During upgrade, the prefix-based MAC allocation scheme configuration is not migrated to the target vCenter

Due to an issue with the configuration path, the prefix-based MAC allocation scheme configuration might not be migrated to the target vCenter during an upgrade.

This issue is resolved in this release.

PR 3486798: ESXi host update or upgrade fails with errors for running out of memory

When an ESXi host enters maintenance mode, it might not clear the resource pool mirror and reservations for the mirror before the evacuations of the last VM are not freed. This leads to insufficient memory being available for upgrade or update, especially if the last VM that is evacuated has a large reservation, such as tens of GBs. In the backtrace, you see an error such as `Admission failure in path: host:system:kernel:stagebootbank.`

This issue is resolved in this release.

vSAN Issues

PR 3419045: vSAN tasks fail with NotSupported exception

In vSAN HCI with datastore sharing environment (formerly HCI Mesh), a vSAN datastore that belongs to one vSAN cluster can be mounted on hosts of other clusters. Such hosts provide only compute and not storage, and might not even have vSAN active. In the Site Recovery Manager reprotect workflow, if a certain API call is made to a host with no active vSAN, the call ends with a `NotSupported` exception. If such a call is made to a vSAN-enabled compute-only host, then you see no error, but the call does not return any results.

This issue is resolved in this release. The fix makes sure API calls for the SRM reprotect workflow to pick up only hosts with active vSAN.

Known Issues

vCenter and vSphere Client Issues

If the vCenter certificate mode is set to thumbprint or custom, you cannot export logs by using the vSphere Client

If for some reason the advanced setting `vpxd.certmgmt.mode` in a vCenter instance is set to `thumbprint` , which is recommended only as a fallback option, or `custom` , you cannot export logs by using the vSphere Client.

Workaround: Change the `vpxd.certmgmt.mode` setting to `vmca` .

You cannot upload log packages to a VMware service request by using the vSphere Client

You cannot upload log packages to a VMware service request by navigating in the vSphere Client to **Administration > Support > Upload File to Service Request**. Instead, you see a link to a KB article that provides steps to upload log bundles in the Broadcom Support Portal. This is expected.

Workaround: Follow the steps in Uploading files to cases on the Broadcom Support Portal.

Security Issues

Update Manager Download Service (UMDS) stores proxy passwords in plain text

When UMDS accesses a VMware online depot by using a proxy, if you have configured a proxy password, it is stored in the configuration as plain text, which in some environments might be a security concern.

Workaround: Instead of configuring a password, you can pass the password every time you run a `Downland (-D)` and `Re-Download (-R)` command. For example, `./vmware-umds -D --proxy-username "<your_username>" --proxy-password "<your_password>" --proxy-port 80 --proxy-ip 1.1.1.1` .

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:
```

`IP: 10.0.0.10 ...`

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405` . The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify` .

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the`/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the`/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR).

Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the

setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3w Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Resolved Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3w | 29 SEP 2025 | ISO Build 24927011 Check for additions and updates to these release notes.

What's New

- This release resolves CVE-2025-41250. For more information on this vulnerability and its impact on Broadcom products, see VMSA-2025-0016.

Patches Contained in This Release

Patch for VMware vCenter 7.0 Update 3w

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02500-24927011-patch-FP.iso
Build	24927011
Download Size	6.23 GB
md5sum	0c9673c05cc9a92b80e4c4d3083f3979
sha256checksum	a1271853908a96d881e5e36fc70d2c1cc809b21fe3be38db29016588fdd9097c
PRs fixed	N/A
CVEs	CVE-2025-41250

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Security Issues

- This release resolves CVE-2025-41250. For more information on this vulnerability and its impact on Broadcom products, see VMSA-2025-0016.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.

2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405` . The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify` .

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the`/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`

- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation..`

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

vCenter Server Update and Patch Releases

VMware vCenter Server 7.0 Update 3w Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Resolved Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3w | 29 SEP 2025 | ISO Build 24927011

Check for additions and updates to these release notes.

What's New

- This release resolves CVE-2025-41250. For more information on this vulnerability and its impact on Broadcom products, see VMSA-2025-0016.

Patches Contained in This Release

Patch for VMware vCenter 7.0 Update 3w

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02500-24927011-patch-FP.iso
Build	24927011
Download Size	6.23 GB
md5sum	0c9673c05cc9a92b80e4c4d3083f3979
sha256checksum	a1271853908a96d881e5e36fc70d2c1cc809b21fe3be38db29016588fdd9097c
PRs fixed	N/A
CVEs	CVE-2025-41250

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Security Issues

- This release resolves CVE-2025-41250. For more information on this vulnerability and its impact on Broadcom products, see VMSA-2025-0016.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On

certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**

- Copy the IP displayed in the **Control Plane Node IP Address** tab.
- You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
  Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.

2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...
Status: Running
IP: 10.0.0.10
IPs:
IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs`. Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS

1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.`.

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi

6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

`RuntimeError: unidentifiable C++ exception.`

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.

2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules

to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.

- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed` .

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation..`

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.

- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3v Release Notes

This document contains the following sections

- Introduction
- What's New
- Upgrade Notes
- Patches Contained in This Release
- Resolved Issues
- Known Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3v | 20 MAY 2025 | ISO Build 24730281 Check for additions and updates to these release notes.

What's New

- For vCenter Server 7.0 Update 3v updates, see the **Resolved Issues** and **Known Issues** sections.
- For vSphere Supervisor updates, see the vSphere Supervisor Release Notes.
- For Photon OS updates, see VMware vCenter Server Appliance Photon OS Security Patches.

This release resolves CVE-2025-41225. For more information on this vulnerability and its impact on Broadcom products, see VMSA-2025-0010.

Prefix-Based MAC Address Allocation by the vCenter GUI Installer and CLI:

vCenter 7.0 Update 3v adds the option to use prefix-based allocation to specify an OUI other than the default one 00:50:56 by Broadcom, or to introduce Locally Administered MAC Addresses (LAA) for a larger address space, by using either the vCenter GUI installer or the CLI installer. After deploying a vCenter instance, you can use the vSphere Client to switch between the available allocation schemes.

Upgrade Notes

Upgrading from vCenter 7.0 Update 3v to vCenter 8.0 Update 3e is not supported due to back-in-time release restrictions. For more information, see KB 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3v

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02400-24730281-patch-FP.iso
Build	24730281
Download Size	6686.0 MB
md5sum	33bb110f457ec1d06054cb4362476c22
sha256checksum	00d688b44ff746e59ba9c5cf60d4c6dc791ba70814f46102795f506717973ef4
PRs fixed	3404100, 3404108, 3471234, 3503319, 3484455, 3484244, 3245536, 3426087, 3473337, 3407726, 3384385, 3418166, 3367090, 3444766, 3468763, 3486798, 3419045
CVEs	CVE-2025-41225

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

vCenter and vSphere Client Issues

PR 3404100: vCenter performance stats shows incorrect aggregate values when the data is rolled up to the daily partition

Without date rounding logic, the partition index might start at a random hour instead of 00:00:00, leading to incorrect aggregate values when the data is rolled up to the daily partition.

This issue is resolved in this release.

PR 3404108: Rollup processing of performance stats data in vCenter occurs only by the average rollup type

In vCenter performance statistics, you see only the average value of each duration, regardless if the rollup type is different, such as summation or latest.

This issue is resolved in this release.

PR 3471234: Smart card authentication on vCenter intermittently fails with the error "Unable to validate submitted credentials"

The Certificate Revocation List (CRL) cache updates hourly and if you log in to vCenter by using a smart card during such an hourly cycle in which the old CRL is expired but no new CRL is downloaded, the login fails. Since this is a corner case, smart card authentication on vCenter intermittently fails and in the vSphere Client, you see the error `Unable to validate submitted credentials.`

This issue is resolved in this issue.

PR 3503319: The vpxd service fails because the Guest OS customization API requires IPv4 settings

When you use API to create a Guest Customization Specification and customize the guest OS of a virtual machine, you might need to enter IPv4 settings in the specification or the vpxd service fails with a core dump.

This issue is resolved in this release.

PR 3484455: Distributed Resource Scheduler (DRS) fails to migrate an encrypted VM with an error for missing [Cryptographic operations > Migrate] privileges

In some cases, when DRS schedules to migrate an encrypted VM, it might use the context of a user without `Cryptographer.Migrate` privilege and migration fails with an error in the vSphere Client such as: `Permission to perform this operation was denied. You do not hold privileges "virtual machine vm-xx : [Cryptographic operations > Migrate].`

In the vpxd.log, you see error messages such as:

```
YYYY-MM-DDThh:mm:ss.472Z info vpxd[06061] [Originator@6876 sub=drsExec opID=<op_id>]
Executing DRM recommended vMotion in [vim.ClusterComputeResource:domain-c<id>,esxi_name],
migrating [vim.VirtualMachine:vm-<vm_id>,vm_name] from vim.HostSystem:host-<src_id> to
vim.HostSystem:host-<dstn_id>……..
```

```
YYYY-MM-DDThh:mm:ss.494Z info vpxd[06061] [Originator@6876 sub=pbm opID=<op_id>-01] pre
migrate callback is skipped - for cached from pre migrate check reason
```

```
YYYY-MM-DDThh:mm:ss.494Z warning vpxd[06061] [Originator@6876 sub=CryptoManager
opID=<op_id>-01] The session xx-yy-zz of user DOMAIN\user_name does not have privilege
Cryptographer.Migrate on entity [vim.VirtualMachine:vm-<vm_id>,vm_name].
```

This issue is resolved in this release.

PR 3484244: A rare race condition might cause repeating failovers due to a failure of the vCenter vpxd service or the vSphere Client becoming unresponsive

A rare race condition during a VAPI call from the vpxd service to a virtual machine that coincides with the deletion of a `VirtualMachine` object might cause the vpxd service to fail. As a result, you see repeating failovers or the vSphere Client might become unresponsive.

This issue is resolved in this release.

PR 3245536: When an ESXi host has multiple management IP addresses, in some vSphere Client workflows you might see a "Host not reachable" error

You can assign multiple management IP addresses to a single ESXi host and it is not necessary that all IP addresses are reachable from vCenter at any time. However, if vCenter picks a currently unreachable IP during a workflow that you run from the vSphere Client, such as a remediation precheck, the task might fail with a `Host not reachable` error.

This issue is resolved in this release.

Networking Issues

PR 3351967: Stale NSX properties from ESXi hosts that vCenter might use can cause various networking issues

In some cases, vCenter might retrieve NSX properties from ESXi hosts, save them on the vCenter database and push these NSX properties back to ESXi hosts in various scenarios that can cause the following issues:

1. A virtual switch gets out of sync because vCenter pushes stale NSX properties to an ESXi host.
2. You cannot remove the NSX VIB after you remove a transport node, because vCenter pushes NSX properties back to the virtual switch.
3. After an ESXi host reboot, vCenter feeds stale NSX properties back to the virtual switch.
4. NSX cannot start on a virtual switch due to stale NSX properties.

Logs are different in each case, but you can confirm the issue by checking the `VPX_DVS_BLOB` table in the vCenter DB. If you see NSX properties in the `VPX_DVS_BLOB` table, the issue exists. Look for properties such as:

`com.vmware.nsx.kcp.enable`

`com.vmware.nsx.spf.enabled`

`com.vmware.nsx.vdl2.enabled`

`com.vmware.vswitch.disabled`

`com.vmware.host.feature.container`

`com.vmware.nsx.ens.loadbal`

`com.vmware.nsx.ens.overlayl2flow`

This issue is resolved in this release.

PR 3426087: You see duplicate routes in the Netplan configuration file after guest OS customization on Ubuntu VMs

For Ubuntu releases that support the Netplan utility for configuring networking on a Linux system, when you deploy an Ubuntu VM and customize it with both IPv4 and IPv6 gateways, the Netplan configuration file `/etc/netplan/99-netcfg-vmware.yaml` of the guest OS contains two route sections under a single network interface.

This issue is resolved in this release. With the fix, customizing an Ubuntu VM with both IPv4 and IPv6 gateways creates a single route section for each NIC in the Netplan configuration file, and adds the corresponding IPv4 and IPv6 gateways of the NIC to its route section.

PR 3473337: In the vSphere Client, you still see an NSX overlay segment after deleting it from the NSX Manager

When adding NSX port groups on a vCenter system, vCenter uses an API call to push the port groups to ESXi hosts, but in some cases the call does not complete on all hosts, if a host is temporarily disconnected for example. As a result, from

vCenter perspective, all port groups exist, but from ESXi hosts perspective, some might not exist. Consequently, when you try to delete an NSX overlay segment from the NSX Manager, it still shows in the vSphere Client, because not all port groups can be removed.

This issue is resolved in this release.

PR 3407726: If the Key Management Server (KMS) sends a response not in Key Management Interoperability Protocol (KMIP) format, the vpxd service might fail

In rare cases, KMS might send a response that does not follow the KMIP protocol, which leads to the use of an invalid address in analyzing the response and in turn causes the vpxd service to fail.

This issue is resolved in this release.

PR 3384385: The vpxd service fails after the Mobility Agent (MA) host for VMware HCX is reconnected or redeployed

When you reconnect or redeploy the MA service, which is the data proxy for vSphere vMotion in HCX between onprem and cloud migrations, as a host object in vCenter, the vpxd service might fail due to duplicate entries in the vCenter database. In the vpxd log, you see messages such as `ODBC error: (23505) - ERROR: duplicate key value violates unique constraint "pk_vpx_nw_assignment.`

This issue is resolved in this release.

PR 3418166: You don't see newly created NSX Distributed Virtual port groups on some ESXi hosts

When multiple ESXi hosts join a new transport zone, a race condition in the vCenter host sync handler might cause some ESXi hosts to fail saving the new transport zones configuration. As a result, you don't see newly created NSX Distributed Virtual port groups in the new transport zone on such hosts.

This issue is resolved in this release.

Miscellaneous Issues

PR 3367090: Changes in the authorization roles on an ESXi host are not persistent across reboots

Due to an issue with saving changes to the underlying storage, modifications of the authorization roles on an ESXi host, such as adding a privilege, might not persist across reboots.

This issue is resolved in this release.

PR 3444766: vCenter CPU utilization reaches 100% and the vCenter system becomes slow or unresponsive

After several days of uptime, due to an issue with the Apache HttpCore library, the vCenter CPU utilization by the `vsphere-ui` service might reach 100% and the vCenter system becomes slow or unresponsive.

This issue is resolved in this release.

Upgrade Issues

PR 3468763: During upgrade, the prefix-based MAC allocation scheme configuration is not migrated to the target vCenter

Due to an issue with the configuration path, the prefix-based MAC allocation scheme configuration might not be migrated to the target vCenter during an upgrade.

This issue is resolved in this release.

PR 3486798: ESXi host update or upgrade fails with errors for running out of memory

When an ESXi host enters maintenance mode, it might not clear the resource pool mirror and reservations for the mirror before the evacuations of the last VM are not freed. This leads to insufficient memory being available for upgrade or

update, especially if the last VM that is evacuated has a large reservation, such as tens of GBs. In the backtrace, you see an error such as `Admission failure in path: host:system:kernel:stagebootbank`.

This issue is resolved in this release.

vSAN Issues

PR 3419045: vSAN tasks fail with NotSupported exception

In vSAN HCI with datastore sharing environment (formerly HCI Mesh), a vSAN datastore that belongs to one vSAN cluster can be mounted on hosts of other clusters. Such hosts provide only compute and not storage, and might not even have vSAN active. In the Site Recovery Manager reprotect workflow, if a certain API call is made to a host with no active vSAN, the call ends with a `NotSupported` exception. If such a call is made to a vSAN-enabled compute-only host, then you see no error, but the call does not return any results.

This issue is resolved in this release. The fix makes sure API calls for the SRM reprotect workflow to pick up only hosts with active vSAN.

Known Issues

vCenter and vSphere Client Issues

If the vCenter certificate mode is set to thumbprint or custom, you cannot export logs by using the vSphere Client

If for some reason the advanced setting `vpxd.certmgmt.mode` in a vCenter instance is set to `thumbprint`, which is recommended only as a fallback option, or `custom`, you cannot export logs by using the vSphere Client.

Workaround: Change the `vpxd.certmgmt.mode` setting to `vmca`.

You cannot upload log packages to a VMware service request by using the vSphere Client

You cannot upload log packages to a VMware service request by navigating in the vSphere Client to **Administration > Support > Upload File to Service Request**. Instead, you see a link to a KB article that provides steps to upload log bundles in the Broadcom Support Portal. This is expected.

Workaround: Follow the steps in Uploading files to cases on the Broadcom Support Portal.

Security Issues

Update Manager Download Service (UMDS) stores proxy passwords in plain text

When UMDS accesses a VMware online depot by using a proxy, if you have configured a proxy password, it is stored in the configuration as plain text, which in some environments might be a security concern.

Workaround: Instead of configuring a password, you can pass the password every time you run a `Downland (-D)` and `Re-Download (-R)` command. For example, `./vmware-umds -D --proxy-username "<your_username>" --proxy-password "<your_password>" --proxy-port 80 --proxy-ip 1.1.1.1`.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On

certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**

- Copy the IP displayed in the **Control Plane Node IP Address** tab.
- You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
  Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.

2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs`. Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS

1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.`.

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi

6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

`RuntimeError: unidentifiable C++ exception.`

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.

2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules

to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   – To edit the `.ovf` file, open it with a text editor.
   – Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.

- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed` .

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.

- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3u Release Notes

This document contains the following sections

- Introduction
- What's New
- Patches Contained in This Release
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3u | 31 MAR 2025 | ISO Build 24614210 Check for additions and updates to these release notes.

What's New

- VMware vCenter Server 7.0 Update 3u serves as a vehicle for VMware vSphere with Tanzu and does not deliver vCenter Server fixes.

Patches Contained in This Release

Patch for VMware vCenter 7.0 Update 3u

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02300-24614210-patch-FP.iso
Build	24614210
Download Size	6701.3 MB
md5sum	3ca90d9abb05a79c1b76ff0c573b0228
sha256checksum	483ec3c8184281e69f720ff11d0ad896fc709b1785ec20409f12360f9a83a629
PRs fixed	3479424
CVEs	N/A

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      ```
      kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify
      ```
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      ```
      kubectl config use-context <namespace_name>
      ```
      and
      ```
      kubectl describe pod <pod_name> -n <namespace_name>
      ```

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10
```

```
IPs:
IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

`RuntimeError: unidentifiable C++ exception.`

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the`/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.

3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error.`

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.

2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR).

Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the

setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3t Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Resolved Issues

Introduction

VMware vCenter Server 7.0 Update 3t | 21 OCT 2024 | ISO Build 24322018 Check for additions and updates to these release notes.

What's New

- This release contains additional fixes that fully address CVE-2024-38812. For more information on this vulnerability and its impact on VMware by Broadcom products, see VMSA-2024-0019.2.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3s Release Notes
- VMware vCenter Server 7.0 Update 3r Release Notes
- VMware vCenter Server 7.0 Update 3q Release Notes
- VMware vCenter Server 7.0 Update 3p Release Notes
- VMware vCenter Server 7.0 Update 3o Release Notes
- VMware vCenter Server 7.0 Update 3n Release Notes
- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes

- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3t

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02200-24322018-patch-FP.iso
Build	24322018
Download Size	6789.2 MB
md5sum	1aa0ab47173db8c1e149b6257e1372e8
sha256checksum	968f3799376ac8ea6883d26e9f1f9850ece9048f8936e6520c020289d6f09f98
PRs fixed	N/A
CVEs	CVE-2024-38812

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Security Issues

This release contains additional fixes that fully address CVE-2024-38812. For more information on this vulnerability and its impact on VMware by Broadcom products, see VMSA-2024-0019.2.

VMware vCenter Server 7.0 Update 3s Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Resolved Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3s | 17 SEP 2024 | ISO Build 24201990 Check for additions and updates to these release notes.

What's New

- This release resolves CVE-2024-38812 and CVE-2024-38813. For more information on these vulnerabilities and their impact on VMware by Broadcom products, see VMSA-2024-0019.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3r Release Notes
- VMware vCenter Server 7.0 Update 3q Release Notes
- VMware vCenter Server 7.0 Update 3p Release Notes
- VMware vCenter Server 7.0 Update 3o Release Notes
- VMware vCenter Server 7.0 Update 3n Release Notes
- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes

- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3s

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02100-24201990-patch-FP.iso
Build	24201990
Download Size	6789.2 MB
md5sum	2cb420786b18aa97faf29bac78c437b5
sha256checksum	04ceab872c4278eaaf3ebffd4d28e421662d7c0c7e49c2f88ebe8bc99093c8a9
PRs fixed	N/A
CVEs	CVE-2024-38812, CVE-2024-38813

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Security Issues

This release resolves CVE-2024-38812 and CVE-2024-38813. For more information on these vulnerabilities and their impact on VMware by Broadcom products, see VMSA-2024-0019.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.`.

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network.` This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

`Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.`

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.

- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.

- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed` .

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.

- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3r Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Resolved Issues
- Known Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3r | 17 JUN 2024 | ISO Build 24026615 Check for additions and updates to these release notes.

What's New

- This release resolves CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0012.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3q Release Notes
- VMware vCenter Server 7.0 Update 3p Release Notes
- VMware vCenter Server 7.0 Update 3o Release Notes
- VMware vCenter Server 7.0 Update 3n Release Notes
- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3r

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.02000-24026615-patch-FP.iso
Build	24026615
Download Size	6789.2 MB
md5sum	fa90aee2a9b6c525552e6762a45ee0f4
sha256checksum	aa490abbe2bf6c45041aea93bdbdcd37d147bbe188ceb85e18ed060b50b85c88
PRs fixed	NA
CVEs	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.02000-24026615-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Security Issues

This release resolves CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0012.

Known Issues

Installation, Upgrade, and Migration Issues

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server

7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs`. Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt`. For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on

the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

PR3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

`Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.`

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.

- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error.`

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   – To edit the `.ovf` file, open it with a text editor.
   – Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.

- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed` .

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.

- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3q Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Resolved Issues
- Known Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3q | 21 MAY 2024 | ISO Build 23788036 Check for additions and updates to these release notes.

What's New

- This release resolves CVE-2024-22274 and CVE-2024-22275. For more information on these vulnerabilities and their impact on VMware by Broadcom products, see VMSA-2024-0011.
- For vCenter Server 7.0 Update 3q updates, see the Resolved Issues and Known Issues sections.
- For VMware vSphere with Tanzu updates, see VMware vSphere with Tanzu Release Notes.
- For Photon OS updates, see VMware vCenter Server Appliance Photon OS Security Patches.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3p Release Notes
- VMware vCenter Server 7.0 Update 3o Release Notes
- VMware vCenter Server 7.0 Update 3n Release Notes
- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3q

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.01900-23788036-patch-FP.iso
Build	23788036
Download Size	6788.2 MB
md5sum	eebf90da955138f7162b0e193346f4b1
sha256checksum	540b1cbbbf2b9cf56207b848f4842ae2613416d1ccc3212c01bc3bf60f5d68ef
PRs fixed	3292249, 3240279, 3258998, 3293293, 3267704, 3259574, 3156019, 3233684, 3258392, 3258978, 3262483, 3267091, 3273009, 3273555, 3277662, 3277750, 3279685, 3280718, 3284410, 3286503, 3292267, 3292286, 3292827, 3294825, 3295340, 3296689, 3297510, 3299100, 3299657, 3300880, 3305047, 3298709, 3239235, 3319921, 3243737, 3307800, 3319732, 3323119, 3297645, 3328809, 3279536, 3296460, 3301460, 3302845, 3235633, 3327450, 3314065, 3265677, 3256964, 3314810, 3327398, 3319082, 3304002, 3388577, 3388766, 3294142, 3299260, 3304411, 3317325, 3317759, 3321888, 3322688
CVEs	CVE-2024-22274, CVE-2024-22275

Download and Installation

Log in to the Broadcom Support Portal to download this patch.

For download instructions for earlier releases, see Download Broadcom products and software.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.01900-23788036-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Installation, Upgrade, and Migration Issues

PR 3322688: vCenter fails to perform scheduled NFS file-based backups after an update

In rare cases, after a vCenter update, scheduled NFS file-based backups might fail with an error in the applmgmt logs such as `PluginError` object has no attribute `errorcode` due to an incorrect reference to a variable.

This issue is resolved in this release.

PR 3299260: In Embedded Link Mode mixed environments, the vmware-sps service fails to start

In Embedded Link Mode environments, where you have nodes of version 7.x or earlier and 8.x, the vmware-sps service might fail to start on a vCenter instance of version 8.x, due to a group membership inconsistency issue after a vCenter update.

This issue is resolved in this release.

PR 3240279: vSphere Lifecycle Manager Depot might contain third-party content along with VMware-published content

If you manage your ESXi hosts by using vSphere Lifecycle Manager baselines, you might see third-party content in the Non-Critical Host Patches baseline. A Non-Critical Host Patches baseline that has third-party content might have wrong driver names and metadata that might cause various issues during the lifecycle management of your hosts.

This issue is resolved in this release. The fix filters system baselines to only show VMware-published content. For more information, see VMware knowledge base article 95501.

PR 3314810: Patching vCenter Server to 7.0 Update 3o might fail due to a specific condition that prevents the ESX Agent Manager (EAM) service to start

If a property file does not have a new line at the end, when a new property is added to such a file during an update operation, the new property is on the same line as the last property in the file. As a result, the EAM service might fail to start and the update cannot complete.

This issue is resolved in this release.

PR 3327398: When you upgrade ESXi hosts by using a host profile for stateless caching, the hosts cannot reconnect to vCenter

When you upgrade ESXi hosts by using a host profile for stateless caching, the ESXi license might be considered invalid during the boot process. As a result, applying the host profile fails and the hosts cannot reconnect to the vCenter instance.

This issue is resolved in this release.

PR 3256964: UEFI iPXE boot is slow

Due to a rare performance issue, UEFI iPXE boot might be slow and take more than 3 minutes.

This issue is resolved in this release.

PR 3299657: Migration of virtual machines with Virtual Trusted Platform Module (vTPM) across vSphere DRS-enabled clusters fails

In the vSphere Client, when you try to migrate VMs with vTPM across DRS-enabled clusters without selecting any hosts, the final step of the wizard fails with an error such as `A DRS fault has occurred while retrieving VM placement recommendations: xvmotionPlacement`. If you use the PlaceVM API to live relocate a VM with a vTPM from one DRS cluster to another DRS cluster, the operation also fails.

This issue is resolved in this release. With the fix you can safely migrate VMs with vTPM across DRS-enabled clusters.

PR 3307722: Patching vCenter Server to 7.0 Update 3o fails with an error for unsuccessful Redhat Package Manager (RPM) installation

In rare cases, during patching of vCenter Server to version 7.0 Update 3o, some dependent RPMs might not be installed during the pre-upgrade stage due to stale entries in the vCenter Server database. As a result, in the Virtual Appliance Management Interface you see the error **Installation of one or more RPMs failed** and the patching operation is not successful.

This issue is resolved in this release.

Networking Issues

PR 3304411: After batch cloning and customizing Windows virtual machines, the VMs network might not be configured

When cloning Windows VMs in bulk, a MAC address conflict might occur, causing vCenter to reassign new MAC addresses to the VMs. As a result, the guest customization process fails to configure properly the VMs network because it cannot match the original MAC address to the corresponding network card.

This issue is resolved in this release.

PR 3258392: You see a black screen after activating the VMware Remote Console (VMRC) proxy service

After you activate the VMware Remote Console, you see a black screen with an error such as `The webmks ticket has expired.` instead of configuration parameters.

This issue is resolved in this release.

PR 3280718: A VM cannot reconnect to a vSphere Distributed Switch after reverting from a snapshot acquired before it disconnects from the VDS

If you take a snapshot of a virtual machine connected to a VDS, change the port connection to another portgroup, and then connect back to the portgroup of the VDS, the VM cannot reconnect to the VDS when you revert it from the snapshot. The issue occurs due to a possible mismatch of the VM VNIC connection ID.

This issue is resolved in this release.

PR 3262483: Migration of virtual machines on ESXi hosts connected to an NSX segment fails with an error The object or item referred to could not be found

In the vSphere Client, you see an error such as `Operation failed.........The object or item referred to could not be found` when trying to migrate VMs between ESXi hosts that are connected to an NSX segment, previously known as a logical switch.

This issue is resolved in this release.

PR 3277750: You see vNICs mapped to a combination of ESXi host and portgroup identified by nsx.LogicalSwitch:<uuid> instead of the portgroup name

When you delete ports that no longer belong to a given portgroup, the port number parameter for the portgroup might become negative. As a result, you see some vNICs mapped to an ESXi host and some of the deleted ports identified by `nsx.LogicalSwitch:<uuid>` instead of the portgroup name.

This issue is resolved in this release.

PR 3292827: You cannot remove an ESXi host with a VM template from a vCenter system with an NSX Distributed Virtual port group (DVPG)

When you try to remove an ESXi host with a VM template from a vCenter system with a NSX DVPG, the operation might fail with an error such as `vDS port xxx cannot be found` that you see in the vSphere Client. The issue occurs, because when the ESXi host is part of a NSX DVPG, the group is also removed from the vCenter system, and by the time vCenter tries to move the VM template to another host, the host is already disconnected.

This issue is resolved in this release.

Storage Issues

PR 3319082: In the vSphere Client, you see an error and cannot edit VM Storage Policies

In the vSphere Client, when you try to edit **VM Storage Policies**, you might see an error such as `Failed to retrieve data from the server.` In the Storage Policy Service (SPS) logs, you can see the entries related to the `ArrayIndexOutOfBoundsException`. Lack of synchronization for the `SimpleDateFormat()` method across different threads causes the issue.

This issue is resolved in this release.

PR 3301460: You see excessive Storage Profile Service (SPS) logs in the vCenter /storage/log directory

Logs for the Storage Profile Service, such as `sps-access-log` and `sps-external` , produced by services such as the Apache Tomcat Java Servlet for example, might not properly rotate, or compress after rotation, or have no limit on the log file. As a result, unhandled logs fill up the `/storage/log` directory.

This issue is resolved in this release. As part of the fix, the `sps-runtime.log.stderr` takes over the `sps-external` log and you no longer see this file.

PR 3298709: If tasks to reconcile a datastore and to delete a First Class Disk (FCD) run in parallel, you might see storage and memory outage

If you trigger parallel tasks to reconcile a datastore and to delete a FCD, the two tasks might race and cause inconsistencies in the FCD catalog. As a result, you might see the catalog size increasing, the FCD operation slowing down, and even datastore storage and hostd memory outage issues.

This issue is resolved in this release. However, running a reconcile datastore operation while other FCD operations are in progress might cause other issues that are not supported.

PR 3267704: Virtual machines become intermittently unresponsive due to stale First Class Disk (FCD) threads

A rare issue causing FCD threads to take longer than expected might lead to a time out of FCD operations in some environments. As a result, you might see intermittent unresponsiveness of virtual machines.

This issue is resolved in this release.

PR 3267091: You see unusually high CPU usage when you open the Storage DRS recommendations page under the vSphere Client datastore view

In the **Monitor** tab in the vSphere Client datastore view, when you look at the Storage DRS recommendations, you might see unusually high CPU usage, up to 100%. The issue occurs due to a fault search algorithm in the DRS recommendation service.

This issue is resolved in this release.

Miscellaneous Issues

PR 3319732: An ESXi host might fail to exit maintenance mode after a remediation by using the vSphere Lifecycle Manager

In rare cases, if an ESXi host takes long to reconnect to a vCenter instance during a remediation, the vpxd service falsely detects missing heartbeats between the vpxa service on the host and vpxd. As a result, vpxd marks the connection as not active, which leads to a failure for the host to exit maintenance mode.

This issue is resolved in this release.

PR 3277662: You see many errors for HTTP failure due to the waitForUpdates method in the vpx service logs

Canceling the `waitForUpdates()` method is part of the normal workflow when the vpx service waits for a task running on the vpxa or hostd service to complete. However, the canceled call results in a failed HTTP request and subsequently in a log message at the `info` level. In some environments, such messages, which are not requesting any specific action, might significantly load the vpx service logs.

This issue is resolved in this release. The fix lowers the log level to `verbose` in case the fault for the `waitForUpdates()` method is `RequestCanceled` to avoid logging of unnecessary messages in the vpx service logs.

PR 3314065: You see the vCenter storage/core partition filling up with core files of the vmafd service

In rare cases, due to a segmentation fault, you might see core files of the VMware Authentication Framework Service Daemon (vmafd) being generated intermittently and filling up the vCenter `storage/core` partition.

This issue is resolved in this release.

PR 3265677: In the vSphere Client, after refreshing the STS signing certificate, you see errors that Image view from the vSphere Lifecycle Manager is not available for an object

Due to a rare issue, when you refresh the STS signing certificate, the new chain of the STS certificate might not include the full chain of the VMware Certificate Authority (VMCA) certificate. This might cause internal authentication errors. As a result, in the vSphere Client, you see an error such as `View 'Image' from 'Lifecycle Manager' is not available for this object` in the **Updates** tab of an object.

This issue is resolved in this release.

PR 3327450: Even if you set a category for single cardinality, you can assign more than one tag to a virtual machine

In the vSphere Client, when you create a new category with cardinality set to One Tag Only, you still can assign more than one tag to a virtual machine. For example, when you navigate to **Tags and Custom Attributes** > **Assign Tag** and create two tags with the new category, you see both tags assigned, despite the single cardinality rule.

This issue is resolved in this release.

PR 3328809: vCenter Content Library sync might fail due to changed order of processes

In case of parallel changes in several Content Library items, during the sync operation, the priority and execution order of some tasks might change on the subscribed vCenter, leading to a conflict. For example, if you rename and then delete an item, the subscriber library might attempt first to delete it before renaming it, which causes a sync failure on the subscribed vCenter. In the `/var/log/vmware/content-library/cls.log` , you see messages such as:

```
error = TransferError (com.vmware.transfer.transfer_error) => {
```

```
message = Reached the maximum number of retries (10) while attempting to transfer from com.vmware.transfer.impl.HttpClientEndpointImpl@c5f0374. Failing transfer.
```

This issue is resolved in this release.

PR 3296689: The vpxd service might fail after reverting the vCenter VM to a snapshot due to a duplicate key value error

When you revert the vCenter VM to a snapshot of version earlier than 8.0 Update 2, object IDs of existing VMs and such added after creating the snapshot might duplicate and cause the vpxd service to fail. In the `/var/log/vmware/vpxd/vpxd.log` , you see lines such as:

```
ERROR: duplicate key value violates unique constraint "pk_vpx_entity"
```

```
DETAIL: Key (id)=(123456) already exists.;
```

```
Error while executing the query" is returned when executing SQL statement "INSERT INTO VPX_ENTITY (ID,NAME,TYPE_ID,PARENT_ID) VALUES (?,?,?,?)
```

This issue is resolved in this release.

PR 3284410: vSphere Client intermittently becomes unresponsive and reports OutOfMemoryError

Scan results that the vpx service consumes to provide data to the Task Console and the vSphere Client are stored in the vpxd memory and in some environments can cause an out of memory condition. As a result, the vSphere Client becomes unresponsive and in extreme cases, the vpx service might fail.

This issue is resolved in this release. The fix deletes stale scan results from the vpxd memory.

PR 3299100: The vpx service might intermittently fail due to unlimited number of object updates

In cases such as deploying a large-scale virtual desktop infrastructure, when the vpx service handles the update of an unlimited number of objects, the service might fail.

This issue is resolved in this release. The fix handles such large-scale updates in batches of around 100.

PR 3305047: You do not see the "Configure virtual disk digest" and "Recompute virtual disk digest" tasks in the Recent Tasks pane

You might not see tasks related to Content Based Read Cache (CBRC), such as **Configure virtual disk digest** and **Recompute virtual disk digest** in the **Recent Tasks** pane at the bottom of the vSphere Client, even when a task completes successfully.

This issue is resolved in this release. The fix makes sure that CBRC-related tasks display in the **Recent Tasks** pane and the Task Console.

PR 3259574: You see few events in the Events tab in the vSphere Client

In certain environments, domain users might see just a few events in the **Events** tab in the vSphere Client, for example 1 day worth of events. The issue is likely to occur in environments with vSphere Cluster Services enabled, because events related to such objects are restricted for many users and might affect the way vCenter collects events. As a result, the **Events** page does not fully load and the navigation button might be dimmed.

This issue is resolved in this release.

PR 3273009: Standby operations take long on certain servers in a vSphere Distributed Power Management (DPM) environment

In a vSphere environment with vSphere DPM enabled, enter standby operations might take as much as 10 minutes and exit standby operations might take up to 20 minutes on certain servers.

This issue is resolved in this release.

PR 3279685: You see blank Events page in the vSphere Client

In the vSphere Client, when you navigate to **Monitor** > **Tasks and Events** > **Events** for a given object, you see a blank page. The issue occurs intermittently when a session reaches the maximum number of event history collectors.

This issue is resolved in this release. The fix makes sure that event history collectors are correctly released after fetching an event.

Virtual Machines Management Issues

PR 3323119: Changing an Input/Output Operations Per Second (IOPS) limit might cause a significant drop in the I/O throughput of virtual machines

When you edit an existing IOPS limit based policy on Storage I/O Control (SIOC) by using Storage Policy Based Management (SPBM), you might see significantly slower VM performance. Normally, when you set an SPBM policy, IOPS limits are handled by an I/O filter, while mClock, the default I/O scheduler, handles reservations and shares. Due to a logic fault, when you change an existing IOPS limit, I/Os might throttle at the mClock scheduler instead at the I/O filter. As a result, I/Os get with a significant delay to the I/O filter which causes a drop in the I/O throughput of virtual machines.

This issue is resolved in this release. The fix makes sure that IOPS limits, reservations and shares are honored whenever a new policy is created, edited or restored back to datastore defaults.

PR 3258978: In the vSphere Client, you see VMware Tools version status on some VMs with the string .text appended

In the vSphere Client, some virtual machines might display the VMware Tools version status with the string `.text` appended, for example `Running, version:12325.text`. This issue is specific for ESXi hosts with GuestStore enabled. Due to the same issue, you might see reports in Aria Operations that certain VMs have no VMWare Tools installed.

This issue is resolved in this release. The fix makes sure that in the vSphere Client you see the VMware Tools version status correctly, without the string `.text` appended. In Aria Operations, you might still see reports that VMs have no VMWare Tools installed, but migrating the VMs to a different ESXi host typically resolves the issue.

PR 3297510: You see the same Worst Case Allocation value of virtual machines for both CPU and Memory

In the vSphere Client, when you monitor **Resource Pool** > **Resource Settings**, you might see the **Worst Case Allocation** value identical for both the CPU and Memory metrics.

This issue is resolved in this release.

PR 3286503: Encrypted virtual machines in a vSphere DRS cluster might power on slowly

Power-on of encrypted VMs in a DRS-enabled cluster might take more than 90 seconds because of the time it takes to synchronize the VM encryption keys to each ESXi host within the cluster.

This issue is resolved in this release. The fix removes redundant encryption key synchronizations.

Security Issues

PR 3292267: vCenter GUI installer and VMware Cloud Gateway installer are no longer compatible with Windows Server 2012 and Windows Server 2012 R2

Since Windows Server 2012 and Windows Server 2012 R2 reached end of support on October 10, 2023, vCenter GUI installer and VMware Cloud Gateway installer are no longer compatible with these versions.

This issue is resolved in this release.

vSAN Issues

PR 3239235: You cannot remove IP settings in the vSAN File Service Domain wizard

In the vSphere Client, when you open the **File Service Domain** wizard, the affinity site selection area overlaps the button to remove IP settings and you cannot click the button. The issue affects only vSAN Stretched Cluster environments.

This issue is resolved in this release.

PR 3295340: You see vSAN health alert Unable to fetch key provider details on host on multiple ESXi hosts

When the vSAN health service connects to the vAPI of the vpxd service, it creates a new configuration stub for each connection, which might cause breaching of the session count limit. As a result, the vSAN health service triggers the alert `Unable to fetch key provider details on host` on multiple ESXi hosts.

This issue is resolved in this release. The fix creates a cache of the vpxd vAPI configuration stub and reuses it for consecutive connections.

vSphere Cluster Services Issues

PR 3156019: OVA deployment from URL might fail with the error Unable to retrieve manifest or certificate file

For large OVA files that do not contain a certificate, during the PULL-based deployment by using a URL, the certificate retrieval process times out. As a result, the deployment fails with the error message `Unable to retrieve manifest or certificate file.`

This issue is resolved in this release.

vCenter Server and vSphere Client Issues

PR 3235633: You see duplicate endpoints for the Active Directory after a domain repoint

When you repoint a vCenter Server instance to a new domain with a standalone vCenter Server instance, you might see duplicate endpoints for the Active Directory.

This issue is partially resolved in this release.

PR 3319921: Login and vSphere Client sessions might be affected from connectivity issues between VMware Cloud Gateway and VMware Cloud

With vSphere 7.0 Update 3q, if you use vSphere 7.0 Update 3o or later, you no longer need to honor the 45-minute window of vSphere Client sessions to maintain connectivity between VMware Cloud Gateway and VMware Cloud. If your vSphere system is of version earlier than vSphere 7.0 Update 3o, after upgrading to 7.0 Update 3q, you can log in to the vSphere Client at any time and see no error for loss of connectivity between VMware Cloud Gateway and VMware Cloud.

This issue is resolved in this release.

PR 3273555: You see the error "No matching request found for WebSSO response" after the vSphere Client log in page is idle for a long period

When you log in to the vSphere Client and do not refresh the log in page for more than 30 minutes, you see a blue screen with a red banner that displays the following message:

```
[400] An error occurred while processing the authentication response from the vCenter Single Sign-On server. Details: No matching request found for WebSSO response
```

If you click the **Back to login screen** link in the banner, you successfully log back in to vCenter.

This issue is resolved in this release. The fix removes the error banner and automatically logs back to vCenter when the current relay state token expires.

PR 3293293: For Windows Server 2022 VMs, you see status Unknown for VMware Tools and VM Hardware Compatibility in the Updates tab of the vSphere Client

For Windows Server 2022 virtual machines, you might see status **Unknown** for **VMware Tools** and **VM Hardware Compatibility** in the **Updates** tab on the VM, Host, and Cluster level of the inventory in the vSphere Client.

This issue is resolved in this release.

PR 3302845: In the vSphere Client, you might not see all tasks under Monitor > Tasks and Events > Tasks

Due to a limitation in the back-end process for collecting active tasks, in the vSphere Client, under **Monitor** > **Tasks and Events** > **Tasks**, you might not see all tasks for a vCenter object.

This issue is resolved in this release.

PR 3297645: You see a compatibility error for some client plug-ins on the Client Plugins page in the vSphere Client

Due to an issue with the remote plug-in multi-manifest support, in the vSphere Client, under **Administration** > **Solutions** > **Client Plugins**, you see an error such as `The plug-in is incompatible with the current vSphere Client version...` for some client plug-ins.

This issue is resolved in this release.

PR 3294825: Log in to the vSphere Client fails with an error for maximum number of sessions

In large vCenter Embedded Linked Mode environments, if multiple users, who do not have permissions to log in to any of the vCenter instances in the linked group, try to log in, the vSphere Client might reach the maximum number of allowed HTTP sessions. As a result, you see the error page `[403] The maximum number of sessions has been exceeded.`.

This issue is resolved in this release.

PR 3233684: You do not see health status and version information for a newly added vCenter instance in the System Configuration tab

In the vSphere Client, when you add a new vCenter instance to a vCenter Enhanced Linked Mode group, you might see status **Unknown** in the **Node Health**, **Uptime** and **Version** columns in the **Administration**> **System Configuration** tab. The issue occurs because vSphere Client caches the list of services info that feeds the **System Configuration** view and does not update the cache when you add a new vCenter instance.

This issue is resolved in this release. The fix makes sure that vSphere Client refreshes the list of services when you add a new vCenter instance.

PR 3292286: Log in to the vSphere Client intermittently fails

In large environments where the vsphere-ui service handles multiple concurrent tasks and a single task request might exceed 20 MB, the service might run out of memory and fail. As a result, log in to the vSphere Client intermittently fails.

This issue is resolved in this release.

PR 3258998: Check new notifications tasks pile up in the Tasks list

In the vSphere Client, you see new **Check new notifications** tasks appearing on regular intervals in the task list under **Monitor** > **Tasks and Events** > **Tasks**.

This issue is resolved in this release. The fix removes the **Check new notifications** task.

CIM and API Issues

PR 3300880: Content Library API calls from the vSphere Client API Explorer tab might fail with an error for invalid argument

An issue with building the query parameters when you invoke some of the Content Library APIs by using the **API Explorer** tab under **vSphere Client home page** > **Developer Center**, might cause the call to end with an error. For example, if you run a command such as `GET /api/content/library/item?library_id`, you might see an error such as `Invalid value for property with name: library_id.`

This issue is resolved in this release.

vSphere Lifecycle Manager Issues

PR 3243737: Export of a vSphere Lifecycle Manager image fails with an error that your connection is not secure

In the vSphere Client, when you export a vSphere Lifecycle Manager image, the task might fail with an error such as `Connection is not secure`, regardless of the browser. The issue occurs due to a missing VIB metadata schema file in some environments.

This issue is resolved in this release.

High Availability and Fault Tolerance Issues

PR 3294142: vCenter Server High Availability fails to configure in a multi-subnet environment

If the IP address string of passive and witness nodes is shorter than the length of the IP address of the active node in a multi-subnet environment, the vCenter Server High Availability fails to configure.

This issue is resolved in this release.

PR 3304002: VMware vSphere High Availability configuration takes long after a vCenter upgrade

Certain conditions during the restart of the vpxd service might cause inconsistencies during vSphere HA configuration and take up to 15 minutes to resolve.

This issue is resolved in this release. The fix resolves the underlying issues for possible vSphere HA configuration inconsistencies after a vCenter upgrade and removes the 15 min delay.

PR 3279536: vSphere High Availability (HA) reconfiguration might time out due to a delay in image compliance check tasks

After an ESXi update, a race condition might cause the image compliance check to take longer than usual and lead to issues such as time out of the vSphere HA reconfiguration after the update.

This issue is resolved in this release.

PR 3307800: You see a vCenter High Availability primary node fail over without any errors

When issues with the main thread or a system failure cause a failover of a vCenter High Availability primary node, the system restarts, but you might see no errors in the vCenter Service Life Cycle Management logs. The issue occurs because of a `LINUX_REBOOT_CMD_RESTART` call immediately after the restart without a sync, which prevents the proper logging of error messages. As a result, you see no errors after the restart and the vCenter High Availability primary node failover seems unexpected.

This issue is resolved in this release. The fix makes sure that vCenter Service Life Cycle Management logs the error messages properly after a vCenter High Availability primary node restart from a failover.

Guest OS Issues

PR 3321888: After a VM guest customization by using vAPI, all NICs are connected

When you customize the guest OS of a virtual machine by using vAPI, even if certain NICs have their `start_connection` option set to `false` to prevent them from connecting to the network upon VM startup, all NICs are automatically connected after the VM boots. This issue does not occur when running guest customization by using the vSphere Client.

This issue is resolved in this release.

Known Issues

vCenter Server and vSphere Client Issues

PR 3235633: You see duplicate endpoints for the cs.registry after a domain repoint

When you repoint a vCenter Server instance to a new domain with a standalone vCenter Server instance, you might see duplicate endpoints for the cs.registry.

Workaround: None

Upgrade Issues

Patching vCenter to version 7.0 Update 3q might fail due to unsupported TLS ciphers in the Envoy proxy configuration

During the update of a vCenter instance to version 7.0 Update 3q, some services might fail to start due to custom configuration of the TLS cipher suites in the file `/etc/vmware-rhttpproxy/config.xml` . As a result, in the vSphere Client you see a warning such as `An error occurred while starting service 'vpxd-svcs'` and the process fails. If you use the Virtual Appliance Management Interface, you see an error such as `Installation Failed - Exception occurred in postInstallHook.`

Workaround: See KB 369485 for steps how to reset the TLS ciphers to their defaults and retry the vCenter update.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**

- Copy the IP displayed in the **Control Plane Node IP Address** tab.
- You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
  Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.

2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs`. Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS

1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.`.

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi

6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

`RuntimeError: unidentifiable C++ exception.`

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly.

However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

PR 3262556: vCenter upgrade fails with "VP last sync time not updated after waiting for 5 minutes after vCenter update"

In rare cases, during a vCenter upgrade, a race condition between vSphere API for Storage Awareness (VASA) providers might cause the upgrade to fail. In the `pod-service.log` file, you see an error such as `vSAN VP last sync time not updated after waiting for 5 minutes after vCenter update.`

This issue is resolved in this release. The fix prevents the race condition.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error`. When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error`.

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   – To edit the `.ovf` file, open it with a text editor.
   – Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  – APD across the same host
  – Cascading APD across the entire cluster
  – Storage issues
  – Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .

6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command `/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3p Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Resolved Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3p | 07 DEC 2023 | ISO Build 22837322 Check for additions and updates to these release notes.

What's New

- VMware vCenter Server 7.0 Update 3p serves as a vehicle for VMware vSphere with Tanzu updates and delivers a bug fix documented in the Resolved Issues section.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3o Release Notes
- VMware vCenter Server 7.0 Update 3n Release Notes
- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes

- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3p

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.01800-22837322-patch-FP.iso
Build	22837322
Download Size	6723.6 MB
md5sum	a392ae892780006a0f2ea4024d07e7eb
sha256checksum	d9007cacd79e89d56681040a8918d28125c26a2f19694303e184a57053dce897

Download and Installation

Download this patch from the Broadcom Support Portal.

For download instructions for earlier releases, see Download Broadcom products and software.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.01800-22837322-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Installation and Upgrade Issues

Patching vCenter Server to 7.0 Update 3o fails with an error for unsuccessful Redhat Package Manager (RPM) installation

In rare cases, during patching of vCenter Server to version 7.0 Update 3o, some dependent RPMs might not be installed during the pre-upgrade stage due to stale entries in the vCenter Server database. As a result, in the Virtual Appliance Management Interface you see the error **Installation of one or more RPMs failed** and the patching operation is not successful.

This issue is resolved in this release.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      ```
      kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify
      ```
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      ```
      kubectl config use-context <namespace_name>
      ```
      and
      ```
      kubectl describe pod <pod_name> -n <namespace_name>
      ```

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:
```

`IP: 10.0.0.10 ...`

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405` . The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify` .

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the`/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
```

```
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed` .

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.

- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

VMware vCenter Server 7.0 Update 3o Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Product Support Notices
- Resolved Issues
- Known Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3o | 28 SEP 2023 | ISO Build 22357613 Check for additions and updates to these release notes.

What's New

NEW: This release resolves CVE-2023-34048 and CVE-2023-34056. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2023-0023.

- **Migration of persistent container volumes between datastores in the vSphere Cloud Native Storage:** Starting with vSphere 7.0 Update 3o, you can migrate persistent container volumes between datastores in the vSphere Cloud Native Storage by using the vSphere Client.
- **Activate retreat mode for vSphere Cluster Services (vCLS) from the vSphere Client:** With vSphere 7.0 Update 3o, you can activate retreat mode on a vCLS cluster by using the **EDIT VCLS MODE** button at **Configure > vSphere Cluster Services > General**.
- For VMware vSphere with Tanzu updates, see VMware vSphere with Tanzu Release Notes.
- For Photon OS updates, see VMware vCenter Server Appliance Photon OS Security Patches.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3n Release Notes
- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3o

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.01700-22357613-patch-FP.iso
Build	22357613
Download Size	6718.0 MB
md5sum	6591318d7c1b10c16f52eb2553c880a0
sha256checksum	cb5e135aa14f0413f7e9f4d013c6fbcba5a65e12699fa2ba40565784b3dd72fb

Download and Installation

Download this patch from the Broadcom Support Portal.

For download instructions for earlier releases, see Download Broadcom products and software.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.01700-22357613-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Product Support Notices

Restoring Memory Snapshots of a VM with independent disk for virtual machine backups is not supported: You can take a memory snapshot of a virtual machine with an independent disk only to analyze the guest operating system behavior of a virtual machine. You cannot use such snapshots for virtual machine backups because restoring this type of snapshots is unsupported. You can convert a memory snapshot to a powered-off snapshot, which can be successfully restored.

Resolved Issues

Security Issues

This release resolves CVE-2023-34048 and CVE-2023-34056. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2023-0023.

If an Internet proxy password contains certain reserved characters, some vSphere Lifecycle Management operations fail

Certain reserved characters in an Internet proxy password, except alphanumeric and dashes, underscores, periods, and tildes, trigger URL encoding, also known as percent-encoding, of the password string, which causes failure of some vSphere Lifecycle Management operations that require access to the Internet through a password-protected proxy. For example, when you click **Select Actions > Sync HCL** on the vSphere Lifecycle Manager home view in the vSphere Client, you see the error `Update HCL data - A general system error occurred` even though a correct proxy server username and password are configured.

This issue is resolved in this release.

Multiple ESXi hosts intermittently lose connectivity but quickly reconnect

If you have an invalid Key Management Server (KMS) configuration in your vCenter system, such as a stale testing instance, the vpxd service periodically tries to connect to that KMS to check its status, which leads to wrong file descriptors. As a result, ESXi hosts lose connectivity. Hosts disconnect one at a time but reconnected automatically after 1 second.

This issue is resolved in this release.

The field organizationalUnitName is required for Secure Sockets Layer (SSL) certificates

Starting from vCenter Server 7.0 Update 3o, if you use the vSphere Automation API, Certificate Manager utility, or Certificate management CLIs as an interface to manage vCenter Server Certificates, you can leave the `organizationalUnitName` field empty. The change does not affect existing workflows for certificate replacement or Certificate Signing Requests (CSRs). The vSphere Client and PowerCLI 12.4 still require data for the `organizationalUnitName` field.

This issue is resolved in this release.

Vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable

Some third-party tools for vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable.

This issue is resolved in this release.

vCenter Server 7.0 Update 3o provides the following security updates:

- Apache Tomcat is updated to version 8.5.89.
- The Spring Framework is updated to version 5.3.27.
- The Jackson package is updated to version 2.15.2.
- The Commons Lang3 software library is updated to version 3.12.0.
- The Commons-Collections4 software library is updated to version 4.4.
- The Commons-Fileupload software library is updated to version 1.5.
- Velocity-Engine-Core is updated to version 2.3.
- The sqlite-jdbc is updated to version 3.42.0.0.
- Protocol Buffers (Protobuf) is updated to version 3.22.3.
- Jetty is updated to version 9.4.51.v20230217.
- See the PhotonOS release notes for open source changes.

vSAN Issues

vCLS VMs are not powered on after vSAN cluster shutdown and restart

During vSAN cluster shutdown, vSAN disables the cluster in ESX Agent Manager (EAM). When EAM service is restarted, it does not power-on the vCLS VMs.

This issue is resolved in this release.

Transient vSAN health check warning: Network configuration is out of sync

vSAN Skyline health might randomly report that network configuration is out of sync. This transient issue occurs when the vSAN health service uses an outdated vCenter configuration to perform unicast check.

This issue is resolved in this release.

Virtual Machine Management

Migrating virtual machines between vCenter instances with Advanced Cross-vCenter vMotion might fail with "VirtualEthernetCardNetworkBackingInfo required property deviceName not set"

If the source and target vCenter instances, either on-prem or cloud, in an Advanced Cross-vCenter vMotion operation have matching networks with identical names for some of the network adapters, the operation might fail with an error such as `VirtualEthernetCardNetworkBackingInfo required property deviceName not set`. The issue does not affect standard cross-vCenter migration of VMs between linked vCenter instances.

This issue is resolved in this release.

In the vSphere Client, some VM virtual hardware settings display in black on a dark background and you cannot clearly see their values

In the vSphere Client, when you open **Edit Settings > Virtual Hardware** for a virtual machine and expand either the **Memory** or **Hard disks** sections, you see numbers displayed in black on a dark background and cannot clearly see the values.

This issue is resolved in this release.

Migrating multiple VMs between datacenters might fail to complete the Select a compute resource validation step

In rare cases, when you migrate many VMs between datacenters, an issue with a property computation might result in failure to complete the validation on the **Select a compute resource step** and you might not be able to perform the migration.

This issue is resolved in this release.

The parent resource pool or vApp might not be preserved when performing scheduled VM migration within the same cluster

When you schedule a task to migrate VMs and the source and destination hosts are in the same cluster, the VMs might move out of the parent resource pool or vApp after the migration completes.

This issue is resolved in this release.

In the vSphere Client, you cannot apply an encryption storage policy to a virtual machine

If a key management server (KMS) cluster that enables virtual machine encryption tasks has connectivity issues, you cannot apply an encryption storage policy to a VM by using Edit VM Storage Policy or Edit VM Settings in the vSphere Client. You also see long loading times, due to the connectivity issue of the KMS cluster.

This issue is partially resolved in this release. You can set an encryption storage policy to a virtual machine by using Edit VM Settings. However, you must fix the connectivity issue of the problematic KMS server or remove it from the key provider to make sure that encryption policies and the vSphere Client wizards work as expected.

In the vSphere Client, the Select all items option might not function properly after a live refresh of the data grid

In the vSphere Client, when you add or modify an entity in a related object list, for example a list of VMs, the task triggers a self-refresh and a consecutive live refresh of the list. As the data grid gets updated twice, the **Select all items** option might not function properly.

This issue is resolved in this release.

You cannot download .vmx files from a vCenter system

If an ESXi host has encryption mode enabled, you cannot download .vmx files from this host even when individual VMs are not encrypted, unless you have Cryptographer.Access privilege on the vCenter system.

This issue is resolved in this release.

vCenter Server and vSphere Client Issues

Special characters such as '%' in the vCenter folder names appear with escaped characters such as '%25'

In some cases, you might see vCenter folder names that contain special characters such as '`%` ' to display incorrectly in the vSphere Client because the special character is escaped. For example, a folder name `My%Folder` displays as `My %25Folder` .

This issue is resolved in this release.

You see names of network adapters in the Virtual Hardware settings screen in the vSphere Client with "%2f" instead of "/"

In the vSphere Client, when you navigate to a virtual machine > **Edit Settings > Virtual Hardware**, you see the names of network adapters with "%2f" instead of "/". For example, `nw10.55.0.0/24` appears as `nw10.55.0.0%2f24` .

This issue is resolved in this release.

If you delete the default Backup job failed or Backup job success alarms in vCenter, you cannot restore them

The general alarms **Backup job failed** or **Backup job success** in vCenter are default alarms and if you delete them, you cannot add them back, because the backup default alerts are not available in the **Add new alarm** drop-down menu.

This issue is resolved in this release. The fix adds **Backup job failed** and **Backup job success** alarms to the **Add new alarm** drop-down menu.

Installation and Upgrade Issues

You cannot migrate only the configuration and inventory of a vCenter by using the vCenter GUI installer

When you perform a vCenter migration by using the GUI installer, if you select only the option **Configuration and Inventory**, you get data for the full list of options, including **Tasks and Events**, and **Performance Metrics**. The issue occurs, because regardless of the selection in the GUI installer, the selection in the backend is for all data.

This issue is resolved in this release.

You see 'VMware directory error[9127]' in the backlog after vCenter upgrade to vCenter 7.x fails

Due to a possible mismatch between the Common Name, `cn` , and the `sAMAccountName` LDAP attribute in a domain controller in your vCenter system, upgrades to vCenter 7.x might fail. In the `/var/log/firstboot` file, you see messages such as: `INFO wcp-firstboot WCP storage user does not exists, create the user` and `VMware directory error[9127]` .

This issue is resolved in this release.

Miscellaneous Issues

You see two SAN entries with the same hostname in a certificate signing request

In rare cases, a Certificate Signing Request (CSR) might contain duplicate SAN entries. This issue has no functional impact and the CSR succeeds in creating a new certificate.

This issue is resolved in this release.

The vCenter syslog service creates duplicated files into the directory /var/log/vmware/esx/HOSTNAME/

After a change in the upstream configuration of the syslog service on your ESXi hosts, you might see duplicate stream files in the source system that pile up to consume extra space in vCenter.

This issue is resolved in this release.

You see a logs for a duplicate vSphere HA entry after a restart of vSphere HA on an ESXi host

When you use the vSphere Client to configure an advanced option for vSphere HA, if the entry contains a space, for example `<unknownStateMonitorPeriod >`, you might see a duplicate entry for the configured property after a restart of vSphere HA. In the`fdm.log` file on the host, you see an error such as:

```
2022-12-05T20:55:58.592Z fdm[2104214]: Upgrade FDM configuration failed with
error:Duplicate child: unknownStateMonitorPeriod.
```

This issue is resolved in this release.

Migration of ESXi 6.x VMs to 7.0 Update 2 and later fails with an error 'Module 'MonitorLoop' power on failed.'

Migrating a 6.x virtual machine to an ESXi host of version 7.0 Update 2 or later by using vSphere vMotion might fail because the destination host requires larger VM overhead memory than the source host. In the backtrace, you see an error such as `Module 'MonitorLoop' power on failed.`.

This issue is resolved in this release. The fix enhances the vSphere DRS advanced option `NewDeltaAlloc`.

You see some vsphere-ui logs not compressed after rotation

Several vsphere-ui logs, such as `catalina.log`, `localhost.log`, `manager.log`, and `host-manager.log`, are not compressed after rotation and you might see lengthy lists of rotated files, if rotation is more frequent, for example daily.

This issue is resolved in this release.

You see false vSphere Client alarms for certificate expiry with negative expiry dates even when you change the system date

This issue occurs in very rare cases, when for some reason the date on your vCenter system is set to a distant future date, relative to which date vCenter certificates display as expired. As a result, you see certificate expiry alarms as expected, because alarms are not designed to consider cases when the vCenter system is set to a future date. vCenter alarms with negative expiry dates continue even after you change the system time to the correct date.

This issue is resolved in this release. The fix makes sure you no longer see certificate expiry alarms after correcting the system date. Best practice is to avoid setting the date on your vCenter system to a distant future date.

VMware Service Lifecycle Manager (vmware-vmon) vMon closes threads of the vpxd service before it succeeds to produce a core dump in case of failure

In rare cases, when a core dump operation takes long, the vmware-vmon service that monitors the health of vCenter services might close threads of the vpxd service before it succeeds to produce a core dump in case of failure. As a result, you cannot investigate the root cause of the vpxd failure.

This issue is resolved in this release.

The vpxd service frequently fails with a dump during a virtual machine migration operation

In rare cases, when the hostd service returns an empty virtual machine layout during a migration operation, the vpxd service might fail with a dump due to a missing null check for virtual machine layouts.

This issue is resolved in this release. The fix adds a null check for VM layout to prevent vpxd failures.

After a vCenter upgrade, SNMP might return the base version instead of the upgraded vCenter version information

After a vCenter upgrade, when you run a `snmpwalk` command to get the vCenter version information, the command might return the base version instead of the upgraded version information.

This issue is resolved in this release.

Core files of the SNMP service fill up the /storage/core directory

The internal buffer that holds the CPU information of a virtual file system in the file `/proc/cpuinfo` might not be correctly calculated and cause many core files of the SNMP service to generate and fill up the `/storage/core` directory.

This issue is resolved in this release. The fix makes sure that the buffer can hold the entire `cpuinfo` file properly.

ESXi hosts randomly disconnect from the Active Directory domain or vCenter due to Likewise memory exhaustion

Memory leaks in Active Directory operations and related libraries, or when smart card authentication is enabled on an ESXi host, might lead to Likewise memory exhaustion.

This issue is partially resolved in this release. For more information, see VMware knowledge base article 78968.

Networking Issues

You cannot filter distributed port groups on the NSX Port Group ID column

In the vSphere Client, when you try to filter distributed port groups on the NSX Port Group ID column, you might see an error such as `Cannot filter by non-filterable property: DistributedVirtualPortgroup/dvpgNsxId` error or you continuously see the ports datagrid display as loading.

This issue is resolved in this release. The fix unblocks filtering, but you still cannot filter by the NSX Port Group ID column.

Storage Issues

vSphere Storage DRS operations with virtual machines fail with an error: The available storage IOPs capacity is not sufficient for the operation

If some VMs in a storage cluster have storage I/O reservations, vSphere Storage DRS might fail to balance the I/O reservations in the cluster and throw and error such as `The available storage IOPs capacity is not sufficient for the operation.`

This issue is resolved in this release. The manual workaround is to set the vSphere Storage DRS advanced option `EnforceIOReservations` to `0`.

The timestamp property of DatastoreInfo object continuously changes and might even take old timestamps

In case of shared datastores, timestamp in the `DatastoreInfo` object can vary from host to host. Timestamps indicate the time at which an ESXi host pulls data such as free space and capacity from the storage stack and different hosts can trigger refresh at different time. During host sync to update the `DatastoreInfo` object, vCenter might get an older timestamp that the one that another host has just sent, and you see a fluctuation in the timestamps.

This issue is resolved in this release.

CIM and API Issues

Some API commands in the Appliance Shell might return unexpected results

Some API commands that you use in the Appliance Shell in vCenter Server to perform various administrative tasks might return unexpected results. For example, the command `com.vmware.appliance.version1.resources.cpu.stats.get` might return:

`Error in method: Operation Failed. (code com.vmware.applmgmt.err_operation_failed)` or

`Error in executing command: 8002.`

Some health-related commands, such as:

- `com.vmware.appliance.version1.resources.load.health.get`
- `com.vmware.appliance.version1.resources.mem.health.get`
- `com.vmware.appliance.version1.resources.storage.health.get`
- `com.vmware.appliance.version1.resources.swap.health.get`
- `com.vmware.appliance.version1.resources.system.health.get`
- `com.vmware.appliance.version1.resources.softwarepackages.health.get`

might return only gray health status.

This issue is resolved in this release.

The integrity_check_machine_account_executor.py tool might time out and you see a non-fatal error message

When you run the vc-support command to collect the log support bundle of a vCenter, you might see a non-fatal error such as: `cmd "/usr/lib/vmware-vmdir/vmdir-tool/integrity_check_machine_account_executor.py" timed out after 1200 seconds due to lack of progress in last 600 seconds (0 bytes read)`. In such cases, you only need to run that script separately to collect the complete output by using the `[--integrityCheck]` option of the `/usr/lib/vmware-vmdir/vmdir-tool/vmdir_tool.py` tool.

This issue is resolved in this release.

Auto Deploy Issues

Stateless ESXi hosts deployed from a Host Profile with a Fixed password configuration might disconnect from vCenter after a reboot

Stateless ESXi hosts that you deploy by using vSphere Auto Deploy might not exit Maintenance Mode after a reboot and you need to set manually the root password to reconnect the hosts to a vCenter. The issue occurs only when you use a Host Profile with a **Fixed password** configuration that does not correctly apply after a reboot of stateless hosts.

This issue is resolved in this release.

In VMware vSphere+, stateless ESXi hosts that you deploy by using vSphere Auto Deploy might fail to boot or connect to a cluster

When you deploy stateless ESXi hosts by using Auto Deploy in an environment with a vSphere+ license, the verification of the license might fail during the host boot. As a result, the host cannot join the designated cluster and get the proper license.

This issue is resolved in this release.

vSphere vMotion Issues

vSphere vMotion operation from a 6.7.x ESXi host with an Intel Ice Lake CPU fails with msg.checkpoint.cpucheck.fail

vSphere vMotion operations by using either the vSphere Client or VMware Hybrid Cloud Extension (HCX) from an Intel Ice Lake CPU host running ESXi 6.7.x fails with an error such as `msg.checkpoint.cpucheck.fail`. In the vSphere

Client, you see a message that cpuid.PSFD is not supported on the target host. In HCX, you see a report such as `A general system error occurred: vMotion failed:.`

This issue is resolved in this release.

Server Configuration Issues

The VMware vSphere Authentication Proxy (vmcam) service intermittently fails to start and you cannot complete a vCenter file-based backup

When you use the vCenter Server Appliance Management Interface (VAMI) to run a file-based backup, you might see an error such as:

```
Invalid vCenter Server Status: All required services are not up! Stopped services:'vmcam'
```

The issue occurs when the vmcam occasionally fails to start due to a possible change in the ownership of the vmcam log file from `/vmcam` to `/root` after a vCenter update.

This issue is resolved in this release. The fix makes sure the vmcam log file is updated with the correct ownership.

When you configure vSphere Cluster Services (vCLS) datastores by using PowerCLI or VMware Aria Automation Orchestrator you see redeployment of vCLS VMs on regular intervals

When you create a custom datastore configuration of vCLS VMs by using VMware Aria Automation Orchestrator, former VMware vRealize Orchestrator, or PowerCLI, for example set a list of allowed datastores for such VMS, you might see redeployment of such VMs on regular intervals, for example each 15 minutes.

This issue is resolved in this release.

Known Issues

Server Configuration Issues

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

vSphere Lifecycle Manager Issues

You cannot edit the VMware vSphere Lifecycle Manager Update Download scheduled task

In the vSphere Client, when you navigate to a vCenter Server instance and select **Scheduled Tasks** under the **Configure** tab, if you select the **VMware vSphere Lifecycle Manager Update Download** task and click **Edit**, you cannot modify the existing settings.

Workaround: You can edit the **VMware vSphere Lifecycle Manager Update Download** task by following the steps in the topic Configure the vSphere Lifecycle Manager Automatic Download Task.

vSAN Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

Virtual Machine Management

Filtering virtual machines based on IP address does not work for VMs with two or more IP addresses

In the vSphere Client, when you filter a Virtual Machines list by IP address, virtual machines with two or more IP addresses, in cases such as two NICs attached or using virtualized IPs, might not appear in the filtered results.

Workaround: Use the search in the vSphere Client Inventory.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs`. Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt`. For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration

will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405` . The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify` .

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the`/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to

virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
```

```
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: `"esxcli system settings advanced remove -o ProductLockerLocation"`

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed` .

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation..`

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

VMware vCenter Server 7.0 Update 3n Release Notes

This document contains the following sections

- Introduction

- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3n | 06 JUL 2023 | ISO Build 21958406
Check for additions and updates to these release notes.

What's New

- VMware vCenter Server 7.0 Update 3n Release Notes serves as a vehicle for the VMware vSphere with Tanzu Release Notes and does not deliver vCenter Server fixes.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3m Release Notes
- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes
- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3n

VMware vCenter Server 7.0 Update 3n serves as a vehicle for the VMware vSphere with Tanzu update as of July 6, 2023 and does not deliver vCenter Server fixes.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.01600-21958406-patch-FP.iso
Build	21958406
Download Size	6666.9 MB
md5sum	fc951c29000b783f89a4bc994460b3b3
sha256checksum	9010a03215ba83241e1f8e528f023eb63f05c8ff05e4e9c1c31a7b19d9bbd039

Download and Installation

To download this patch from VMware Customer Connect, you must navigate to **Products and Accounts** > **Product Patches**. From the **Select a Product** drop-down menu, select **VC** and from the **Select a Version** drop-down menu, select **7.0.3**.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.01600-21958406-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      ```
      kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify
      ```
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      ```
      kubectl config use-context <namespace_name>
      ```
      and
      ```
      kubectl describe pod <pod_name> -n <namespace_name>
      ```

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...
Status: Running
```

```
IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21` , the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find

additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"` .
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network` . This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

`RuntimeError: unidentifiable C++ exception.`

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
```

```
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error` .

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such

cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on

each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation..`

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change

depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

VMware vCenter Server 7.0 Update 3m Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Resolved Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3m | 22 JUN 2023 | Build 21784236 Check for additions and updates to these release notes.

What's New

- This release resolves CVE-2023-20892, CVE-2023-20893, CVE-2023-20894, CVE-2023-20895, and CVE-2023-20896. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2023-0014.
- vCenter Server 7.0 Update 3m delivers a bug fix documented in the Resolved Issues section.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3l Release Notes
- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes

- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3m

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.01500-21784236-patch-FP.iso
Build	21784236
Download Size	6624.1 MB
md5sum	39e4f737ce68a7da9f960c107afd563a
sha256checksum	988efe66206123094d008e6555804d114752e48453bad2a2c5b079b0f858ea29

Download and Installation

To download this patch from VMware Customer Connect, you must navigate to **Products and Accounts** > **Product Patches**. From the **Select a Product** drop-down menu, select **VC** and from the **Select a Version** drop-down menu, select **7.0.3**.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.01500-21784236-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Resolved Issues

Install and Upgrade Issues

vCenter 7.x installation might fail during firstboot with an error for a missing install parameter

While installing vCenter 7.x, you might see the error `cis.exceptions.InstallParameterException` during the firstboot step due to a missing `upgrade.import.directory` install parameter. The error occurs if vCenter does not find the parameter due to VM restarts, or restores to a VM Snapshot without memory before running the firstboot configuration.

This issue is resolved in this release. The fix makes sure that the `upgrade.import.directory` install parameter is correctly passed during vCenter installation.

Known Issues from Prior Releases

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.

2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration.
  This option does not include tasks and events data.

- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in

progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.

3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network`. This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

`Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.`

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.`. However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional

debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.
2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules

to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

You do not see the VLAN ID in the port properties page of a VMkernel network adapter in the vSphere Client

In the vSphere Client, when you follow the path **Host > Add Networking**, after you select a VMkernel network adapter and an existing standard switch, in the **Port properties** page you might not see the VLAD ID. The issue occurs because the VLAN ID component is part of the `network-ui` module, which is lazy loaded and needs a trigger to refresh.

Workaround: Go to **Host > Configure > Networking > Virtual Switches** to trigger the loading of the `network ui` module and the VLAD ID appears.

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is `"/locker/packages/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: `"/vmtoolsRepo" export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/
vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/
interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual
device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error`. When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error`.

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   - To edit the `.ovf` file, open it with a text editor.
   - Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such

cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  - APD across the same host
  - Cascading APD across the entire cluster
  - Storage issues
  - Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.
4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on

each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation..`

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change

depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc.`

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

VMware vCenter Server 7.0 Update 3l Release Notes

This document contains the following sections

- Introduction
- What's New
- Earlier Releases of vCenter Server 7.0
- Patches Contained in This Release
- Product Support Notices
- Resolved Issues
- Known Issues
- Known Issues from Prior Releases

Introduction

VMware vCenter Server 7.0 Update 3l | 30 MAR 2023 | ISO Build 21477706 Check for additions and updates to these release notes.

What's New

- For vCenter Server 7.0 Update 3l updates, see the Resolved Issues and Known Issues sections.
- For VMware vSphere with Tanzu updates, see VMware vSphere with Tanzu Release Notes.
- For Photon OS updates, see VMware vCenter Server Appliance Photon OS Security Patches.

Earlier Releases of vCenter Server 7.0

Features, resolved and known issues of vCenter Server are described in the release notes for each release. Release notes for earlier releases of vCenter Server 7.0 are:

- VMware vCenter Server 7.0 Update 3k Release Notes
- VMware vCenter Server 7.0 Update 3j Release Notes
- VMware vCenter Server 7.0 Update 3i Release Notes
- VMware vCenter Server 7.0 Update 3h Release Notes
- VMware vCenter Server 7.0 Update 3g Release Notes
- VMware vCenter Server 7.0 Update 3f Release Notes
- VMware vCenter Server 7.0 Update 3e Release Notes
- VMware vCenter Server 7.0 Update 3d Release Notes
- VMware vCenter Server 7.0 Update 3c Release Notes
- VMware vCenter Server 7.0 Update 3a Release Notes
- VMware vCenter Server 7.0 Update 3 Release Notes
- VMware vCenter Server 7.0 Update 2d Release Notes
- VMware vCenter Server 7.0 Update 2c Release Notes
- VMware vCenter Server 7.0 Update 2b Release Notes
- VMware vCenter Server 7.0 Update 2a Release Notes

- VMware vCenter Server 7.0 Update 2 Release Notes
- VMware vCenter Server 7.0 Update 1c Release Notes
- VMware vCenter Server 7.0 Update 1a Release Notes
- VMware vCenter Server 7.0 Update 1 Release Notes
- VMware vCenter Server 7.0.0d Release Notes
- VMware vCenter Server 7.0.0c Release Notes
- VMware vCenter Server 7.0.0b Release Notes
- VMware vCenter Server 7.0.0a Release Notes

For internationalization, compatibility, installation, upgrade, open source components and product support notices, see the VMware vSphere 7.0 Release Notes.

For more information on vCenter Server supported upgrade and migration paths, please refer to VMware knowledge base article 67077.

Patches Contained in This Release

Patch for VMware vCenter Server Appliance 7.0 Update 3l

Product Patch for vCenter Server containing VMware software fixes, security fixes, and third-party product fixes.

This patch is applicable to vCenter Server.

Download Filename	VMware-vCenter-Server-Appliance-7.0.3.01400-21477706-patch-FP.iso
Build	21477706
Download Size	6624.2 MB
md5sum	1ae421156adeb9fd531c537a4d80ccbc
sha256checksum	2ed1607c4c02c2d3e2da9ec75ffb784e9ae74d3f47f2c4d077ec771debd9a042

Download and Installation

To download this patch from VMware Customer Connect, you must navigate to **Products and Accounts** > **Product Patches**. From the **Select a Product** drop-down menu, select **VC** and from the **Select a Version** drop-down menu, select **7.0.3**.

1. Attach the `VMware-vCenter-Server-Appliance-7.0.3.01400-21477706-patch-FP.iso` file to the vCenter Server CD or DVD drive.
2. Log in to the appliance shell as a user with super administrative privileges (for example, **root**) and run the following commands:
   - To stage the ISO:
     ```
     software-packages stage --iso
     ```
   - To see the staged content:
     ```
     software-packages list --staged
     ```
   - To install the staged rpms:
     ```
     software-packages install --staged
     ```

For more information on using the vCenter Server shells, see VMware knowledge base article 2100508.

For more information on patching vCenter Server, see Patching the vCenter Server Appliance.

For more information on staging patches, see Stage Patches to vCenter Server Appliance.

For more information on installing patches, see Install vCenter Server Appliance Patches.

For more information on patching using the Appliance Management Interface, see Patching the vCenter Server by Using the Appliance Management Interface.

Product Support Notices

Restoring Memory Snapshots of a VM with independent disk for virtual machine backups is not supported: You can take a memory snapshot of a virtual machine with an independent disk only to analyze the guest operating system behavior of a virtual machine. You cannot use such snapshots for virtual machine backups because restoring this type of snapshots is unsupported. You can convert a memory snapshot to a powered-off snapshot, which can be successfully restored.

Resolved Issues

vSAN Issues

Moving an ESXi host with encryption enabled to a vSAN cluster might fail with a permission error

In the vSphere Client, when you try to move an ESXi host with enabled encryption to an encrypted vSAN cluster, the operation might fail with an error such as `The session <NULL> does not have privilege Cryptographer.RegisterHost on entity.`

This issue is resolved in this release.

You cannot clear vSAN health check: NVMe device can be identified

If the vSAN health check indicates that an NVMe device cannot be identified, the warning might not be cleared after you correctly select the device model.

This issue is resolved in this release.

Virtual Machine Management

Enter Maintenance Mode task fails when you try to perform maintenance on ESXi hosts where instant clones reside

In some cases, when you try to put in maintenance mode the ESXi hosts where instant clones reside, the task might fail with a `ManagedObjectNotFound` error. The issue occurs because some virtual machine objects enqueued for evacuation might be deleted while in-flight.

This issue is resolved in this release.

In the vSphere Client, you can set automatic startup and shutdown of virtual machines on ESXi hosts in a vSphere HA cluster

In the vSphere Client, when you navigate to an ESXi host part of a vSphere HA cluster and follow the route **Configure** > **Virtual Machines** > **VM Startup/Shutdown**, you see a warning `If the host is part of a vSphere HA cluster, the automatic startup and shutdown of virtual machines is disabled.` However, the **Edit** button is not deactivated and when you click it, you can select the option **Automatically start and stop the virtual machines** with the system and complete the automatic startup and shutdown of virtual machines.

This issue is resolved in this release. The fix makes sure that the **Edit** button in the **VM Startup/Shutdown** option is unavailable for ESXi hosts in a vSphere HA cluster.

A vim.fault.Timedout error might occur when a task to create a virtual machine takes longer than 10 min

If the creation of a virtual machine on an ESXi host takes longer than 10 min, the task might fail with a `vim.fault.Timedout` error.

This issue is resolved in this release.

You cannot add Raw Device Mapping (RDM) as an existing disk to a virtual machine

If the VMX file of a VM resides on an NFS or vSphere Virtual Volumes datastore, when you create or edit that VM, you cannot add an RDM as an existing disk. In the vSphere Client, you see a validation error for the newly added disk. If you change the location for the new disk to a VMFS datastore, the validation error disappears, but the operation fails with error such as: `Invalid virtual machine configuration. Storage policy change failure: @&! *@*@(mgs.disklin.INVALIDDISK) The file specified is not a virtual disk.`

This issue is resolved in this release.

vCenter Server and vSphere Client Issues

SNMPv3 polling on a vCenter system might fail after an upgrade to vCenter Server 7.x due to a null request ID

SNMPv3 polling on a vCenter system might fail when a discovery request returns `requestID = 0`. The issue occurs after an update of the vCenter system to vCenter Server 7.x and might be related to RFC compliance.

This issue is resolved in this release.

The vpxd service might fail and generate a core file due to bad authentication data when performing vCenter Server tagging operations

A rare issue with the authentication of the tagging API might cause the vpxd service to fail and generate a core file in the `/var/core` directory. Such failures of the vpxd service might in turn cause unexpected failovers to passive nodes in vCenter Server High Availability environments.

This issue is resolved in this release.

In vCenter Enhanced Linked Mode, you can see vCenter Server systems of version 8.0 from a 7.x vCenter Server instance

If you have a vCenter Enhanced Linked Mode group that contains vCenter Server instances of versions 8.x and 7.x, when you log in to a 7.x vCenter Server instance, in the vSphere Client, you can see vCenter Server systems of version 8.0. Since vCenter Server 8.0 introduces new functionalities, you can run workflows specific to vSphere 8.0 on the 8.0 vCenter Server, but this might lead to unexpected results when run from the 7.x vSphere Client.

This issue is resolved in this release. The fix makes sure that when in Enhanced Linked Mode, you do not see vCenter Server 8.0 instances when you log in to a 7.x vCenter Server instance.

When you shutdown a virtual machine, other VMs also shut down unexpectedly

In rare cases, after migrating some VMs from a VM list, those VMs might erroneously remain as preselected in the list. As a result, any following operation on one of the VMs in the VM list might be executed on the other VMs too. For example, if you migrate some VMs from one cluster to another and shut down a VM in the first cluster, the VMs migrated to the second cluster might also shut down.

This issue is resolved in this release.

Security Issues

vCenter Server 7.0 Update 3l provides the following security updates:

- Eclipse Jetty is updated to version 9.4.50.v20221201.
- The ini4j library is updated to version 0.5.4.
- Apache Tomcat is updated to version 8.5.84/9.0.70.

- The Jackson package is updated to version 2.14.1.
- The sqlite-jdbc is updated to version 3.40.0.0.
- The Spring Framework is updated to 5.3.24.
- See the PhotonOS release notes for open source changes.

vSphere Client stops responding after you reconfigure vSphere HA on a vCenter instance with a Key Management Server (KMS) cluster

When you enable or reconfigure vSphere HA on a vCenter instance with a KMS cluster, the **Hosts and Clusters** tab in the vSphere Client becomes unavailable. You see no clusters, hosts, or VMs until the vpxd process restarts after the KMS cluster is reconfigured on the vCenter instance.

This issue is resolved in this release.

Repeated rekey operation on a powered on encrypted virtual machine with an IDE controller might cause the VM to shutdown

Generally, you can perform a shallow recrypt while a virtual machine is powered on, but in case the VM has an IDE controller, the VM must be powered off before a rekey operation. When you try to rekey a powered on VM with an IDE controller, in the vSphere Client, you see an error message that the reconfiguration failed. If you retry the operation, the VM might power off and you cannot power it on.

This issue is resolved in this release. If you already face the issue and an encrypted virtual machine cannot power on, use the Managed Object Browser (MOB) to find the page of the target VM, for example https://vcip/mob?moid=vm-14, and run the command `CryptoUnlock_Task` . As a result, the VM can be powered on. Power off the VM and retry the rekey operation. Alternatively, you can unregister and register the VM again and retry the rekey in a powered off state.

Vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable

Some third-party tools for vulnerability scans might report the HTTP TRACE method on vCenter ports 9084 and 9087 as vulnerable.

This issue is resolved in this release.

If you use Integrated Windows Authentication (IWA) for vCenter Server authentication, you might not be able to log in to the vCenter Server system because the STS service (vmware-stsd) might fail

If you use IWA for vCenter Server authentication, the STS service might fail during attempts to log in to the vCenter Server system, because the Active Directory might return a `null` LDAP hostname. Logins fail until the STS service restarts.

The`vMonCoredumper.log` file contains entries similar to the following:

```
2022-12-29T07:16:15.305Z In(05) host-12345 Notify vMon about pool-2-thread-4 dumping core. Pid : 3315
```

```
2022-12-29T07:16:15.320Z In(05) host-12345 Successfully notified vMon.
```

```
2022-127-29T07:16:16.785Z In(05) host-12345 Successfully generated core file /var/core/core.pool-2-thread-4.3315.
```

The `hs_err_sts_pid*.log` file contains entries such as:

```
# A fatal error has been detected by the Java Runtime Environment:
```

```
#
```

```
# SIGSEGV (0xb) at pc=0x00007f4d80203d06, pid=3315, tid=0x00007f4ce3d1f700
```

This issue is resolved in this release.

Installation and Upgrade Issues

Users with Administrator role on vCenter Server do not see warnings for clusters with vSphere Cluster Services (vCLS) enabled

vCenter Server 7.0 Update 3e added a new group of vCenter Server Administrators, vCLSAdmin, with reduced privileges that get Read-only access to virtual machines in clusters with vSphere Cluster Services (vCLS) enabled. An issue with updates to vCenter Server 7.0 Update 3e and later prevents automatic refresh of Administrator roles and you might not see the vCLSAdmin group. As a result, warnings of vCLS VMs might not be visible for users with Administrator role on vCenter Server, only for vCenter Single Sign-On Administrators.

This issue is resolved in this release. The fix makes sure you can see the vCLSAdmin group after an update to vCenter Server 7.0 Update 3l and later, so that you can monitor vCLS VMs.

ADFS user groups cannot authenticate to vCenter after an upgrade

ADFS user groups might not be able to authenticate to vCenter after an upgrade due to a possible mismatch between case-sensitive values in the group name.

This issue is resolved in this release. The fix removes the case-sensitive check.

VMware vSphere Update Manager Download Service (UMDS) might not get latest patch metadata files

UMDS is an optional module of vSphere Lifecycle Manager that downloads software metadata, software binaries, and notifications that might not otherwise be available to vSphere Lifecycle Manager. You use UMDS to download latest ESXi patches, but in some cases, the metadata file containing listing of new patches might not be up-to-date. As a result, ESXi hosts cannot identify the latest patch and prevent updates.

This issue is resolved in this release.

Patching to vCenter Server 7.0 Update 3i or 7.0 Update 3j fails when the clienttrustCA.pem file is empty

If your vCenter Server system has smart card authentication enabled and the `clienttrustCA.pem` file at `/usr/lib/vmware-sso/vmware-sts/conf/` is empty, patching to vCenter Server 7.0 Update 3i or 7.0 Update 3j might fail. The issue occurs because during update, the STS service looks for certificates in the `clienttrustCA.pem` file and if the file is empty, the STS service fails. The issue is specific for vCenter Server 7.0 Update 3i and 7.0 Update 3j.

This issue is resolved in this release. If patching to vCenter Server 7.0 Update 3i or 7.0 Update 3j has failed, re-run the upgrade to 7.0 Update 3l to make sure it completes successfully.

Miscellaneous Issues

Relocating a First Class Disk (FCD) attached to a VM to a datastore might result in health status alert and datastore inaccessibility

The **FCDInfo** field that contains the name of a Persistent Volume in its specification might not update in time when you relocate a FCD attached to a VM to a datastore. As a result, the volume might display a red health status and the datastore accessibility is `NotAccessibile` .

This issue is resolved in this release.

After a vCenter upgrade, vSphere HA fails with an error Device or resource busy

After a cluster upgrade, when vCenter restarts, in a short time most of the VMs might be migrated to a small group of the ESXi hosts in the cluster, which leads to a performance downgrade. In the FDM Install error logs on the ESXi hosts, you see a warning such as `rm: can't remove '/tardisks/vmware_f.v00': Device or resource busy` . After a cluster upgrade, while ESXi hosts reconnect to the vpxd service, the Fault Domain Manager (FDM) agent needs some time to become fully operational. If during this time the vSphere DRS component that scans the VM-to-host compatibility finds the FDM agent does not work on a given ESXi host, DRS forces the migration of the VMs to another host for high availability purposes.

This issue is resolved in this release. The fix adds a new grace period mechanism where DRS waits for 10 minutes until migrating VMs out of their current ESXi host, because of the transient compatibility failure. You can configure this grace period by using the advanced option `CompatCheckTransientFailureTimeSeconds` , following this sample:

```
IOPT(COMPAT_CHECK_TRANSIENT_FAILURE_TIME_SECS,
"CompatCheckTransientFailureTimeSeconds",
"Length of time a same host compatibility check failure is tolerated. "
"(-1 -> ignore same host compatibility check failure)", -1, 3600, 600)
```

In the vSphere Client, you do not see the asset tag for some servers

In vSphere Client, when you navigate to **Configure** > **Hardware** > **Overview**, for some servers you do not see any asset tag listed.

This issue is resolved in this release. The fix ensures that vCenter receives either baseboard info (Type2) asset tag or chassis info (Type3) asset tag for the server. You see the chassis info asset tag when the baseboard info asset tag for the server is empty.

The vpxd service intermittently fails with a core dumpd due to a race condition

A rare race condition between threads of the vpxd service might cause the daemon to fail, because one of the threads might access a data member outside the mutex lock. In the backtrace, you see errors such as *`Panic: Memory exceeds hard limit. Panic`* and `ExtensionManagerMo::UpdateExtension use ExtensionWrapper after free` .

This issue is resolved in this release.

In case of network connectivity issues, the Key Management Interoperability Protocol (KMIP) client might cause high CPU usage

In case of a network outage or connectivity issues, unresolved calls to the KMIP server in your vCenter Server system might cause high CPU usage.

This issue is resolved in this release.

Networking Issues

After a vCenter Server VM reboot, the /var/spool/snmp directory might not exist and you do not see some vCenter Server-related SNMP traps

When the SNMP service is enabled and after a vCenter Server VM reboot, the `/var/spool/snmp` directory might not be mounted in time and you cannot see some SNMP traps, such as `hrStorageSize` .

This issue is resolved in this release.

Storage Issues

Higher than actual vSAN storage pool free space estimate might lead to unexpected storage shortages

The `freeSpace` parameter of a vSAN storage pool might not exclude disks with errors and display the unused space estimate as higher than the actual. As a result, you might see unexpected storage shortages. This issue only affects vSAN storage pools.

Workaround: Manually compute the storage capacity by disregarding the `freeSpace` value of disks with errors from the overall storage capacity provided by the `freeSpace` parameter of the storage pool.

If a vmdk file is bigger than 2TB, importing an OVA from a content library fails with an Invalid disk format error

Due to size restrictions, when you try to import an OVA file that contains a vmdk file larger than 2TB from a content library, in the vSphere Client you see an error such as `com.vmware.transfer.streamVmdk.VmdkFormatException: Invalid disk format (capacity too large).`

This issue is resolved in this release. The fix removes size restrictions on the OVA files in content libraries.

CIM and API Issues

The Guest Power API returns 500 Internal Server Error

The Guest Power API, which is a category of executable operations for the vCenter REST APIs, intermittently returns an HTTP 500 error. The issue occurs after a restart of the VPXD service and does not affect SOAP calls.

This issue is resolved in this release.

vCenter might become temporally unresponsive due to a slow client application

A slow client application might create vCenter API calls that in turn create a very large HTTP response. For the time the slow client reads the response, all other API calls to vCenter get blocked. As a result, vCenter becomes temporally unresponsive.

This issue is resolved in this release.

Known Issues

Server Configuration Issues

Due to a default timeout setting of 2 minutes, log in to vCenter instances in Enhanced Linked Mode takes long when any of the vCenters is down

When you have a number of vCenter instances in Enhanced Linked Mode, if one of the instances is down for some reason, such as maintenance, log in to the other instances might take up to 2 minutes, which is the default timeout setting. Changing the timeout property that specifies the wait time for log in to linked vCenter instances is a complex task that requires manually editing the `LinkedVcGroup.login.timeout` property located in `vim-commons-vsphere.properties` . To simlify the task, starting with vCenter Server 7.0 Update 3l, the setting `LinkedVcGroup.login.timeout=120000` moves from `vim-commons-vsphere.properties` to the `webclient.properties` file. Editing this option allows you to reduce the wait time so that if one of the vCenter logins is taking more time, it does not affect the log in time for other instances.

Workaround: Edit `/etc/vmware/vsphere-ui/webclient.properties` and change the value of `LinkedVcGroup.login.timeout` from `120000` to a smaller value in milliseconds, but consider that a value of `<= 0` is an infinite timeout.

You see a message Error retrieving when trying to view the status of Key Management Server (KMS) instances in the vSphere Client

In the vSphere Client, you might see a message `Error retrieving` for several minutes when trying to view Key Management Server (KMS) instances. The issue occurs when a KMS instance in a standard key provider loses connectivity. Until all network requests to the affected KMS time out, which takes around 4 minutes, you cannot see the status of any KMS instance in your system, only the error message for the key provider. After the timeout, you can see the status of all KMS instances.

Workaround: If you see the Error retrieving message, wait for 4 minutes.

Known Issues from Prior Releases

vSAN Issues

Virtual machines lose connectivity due to a network outage in the preferred site

In a vSAN stretched cluster setup, a network outage in the preferred site might cause inaccessibility of all virtual machines in the site. The virtual machines do not fail over to a secondary site. They remain inaccessible until the network outage is restored.

Workaround: None.

vSphere Cluster Services Issues

If all vSphere Cluster Service agent virtual machines in a cluster are down, vSphere DRS does not function in the cluster

If vSphere Cluster Service agent virtual machines fail to deploy or power on in a cluster, services such as vSphere DRS might be impacted.

Workaround: For more information on the issue and workarounds, see VMware knowledge base article 79892.

System virtual machines that support vSphere Cluster Services might impact cluster and datastore maintenance workflows

In vCenter Server 7.0 Update 1, vSphere Cluster Services adds a set of system virtual machines in every vSphere cluster to ensure the healthy operation of vSphere DRS. The system virtual machines deploy automatically with an implicit datastore selection logic. Depending on your cluster configuration, the system virtual machines might impact some of the cluster and datastore maintenance workflows.

Workaround: For more information on the impacted workflows and possible workarounds, see VMware knowledge base articles 79892 and 80483.

Installation, Upgrade, and Migration Issues

Users with Administrator role on vCenter Server do not see warnings for clusters with vSphere Cluster Services (vCLS) enabled

vCenter Server 7.0 Update 3e added a new group of vCenter Server Administrators, vCLSAdmin, with reduced privileges that get Read-only access to virtual machines in clusters with vSphere Cluster Services (vCLS) enabled. An issue with updates to vCenter Server 7.0 Update 3e and later prevents automatic refresh of Administrator roles and you might not see the vCLSAdmin group. As a result, warnings of vCLS VMs might not be visible for users with Administrator role on vCenter Server, only for vCenter Single Sign-On Administrators.

This issue is resolved in this release. The fix makes sure you can see the vCLSAdmin group after an update to vCenter Server 7.0 Update 3l and later, so that you can monitor vCLS VMs.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2d and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.

3. Start the vpxd service.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

The vCenter Upgrade/Migration pre-checks fail with "Unexpected error 87"

The vCenter Server Upgrade/Migration pre-checks fail when the Security Token Service (STS) certificate does not contain a Subject Alternative Name (SAN) field. This situation occurs when you have replaced the vCenter 5.5 Single Sign-On certificate with a custom certificate that has no SAN field, and you attempt to upgrade to vCenter Server 7.0. The upgrade considers the STS certificate invalid and the pre-checks prevent the upgrade process from continuing.

Workaround: Replace the STS certificate with a valid certificate that contains a SAN field then proceed with the vCenter Server 7.0 Upgrade/Migration.

Problems upgrading to vSphere 7.0 with pre-existing CIM providers

After upgrade, previously installed 32-bit CIM providers stop working because ESXi requires 64-bit CIM providers. Customers may lose management API functions related to CIMPDK, NDDK (native DDK), HEXDK, VAIODK (IO filters), and see errors related to **uwglibc** dependency.

The syslog reports module missing, "32 bit shared libraries not loaded."

Workaround: There is no workaround. The fix is to download new 64-bit CIM providers from your vendor.

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is enabled

Patching to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x is blocked when vCenter Server High Availability is active.

Workaround: To patch your system to vCenter Server 7.0 Update 1 from earlier versions of vCenter Server 7.x, you must remove vCenter Server High Availability and delete the passive and witness nodes. After the upgrade, you must re-create your vCenter Server High Availability clusters.

Migration of a 6.7.x vCenter Server system to vCenter Server 7.x fails with an UnicodeEncodeError

If you select the option to import all data for configuration, inventory, tasks, events, and performance metrics, the migration of a 6.7.x vCenter Server system to vCenter Server 7.x might fail for any vCenter Server system that uses a non-English locale. At step 1 of stage 2 of the migration, in the vSphere Client, you see an error such as:

```
Error while exporting events and tasks data: …ERROR UnicodeEncodeError: Traceback (most recent call last):
```

Workaround: You can complete the migration operation by doing either:

- Select the default option **Configuration and Inventory** at the end of stage 1 of the migration. This option does not include tasks and events data.
- Clean the data in the events tables and run the migration again.

If a Windows vCenter Server system has a database password containing non-ASCII characters, pre-checks of the VMware Migration Assistant fail

If you try to migrate a 6.x vCenter Server system to vCenter Server 7.x by using the VMware Migration Assistant, and your system has a Windows OS, and uses an external database with a password containing non-ASCII characters, the operation fails. For example, Admin!23迁移. In the Migration Assistant console, you see the following error:

```
Error:Component com.vmware.vcdb failed with internal errorResolution:File Bugzilla PR to VPX/VPX/vcdb-upgrade
```

Workaround: None

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide the vCenter Single Sign-On password

During an update from vCenter Server 7.x to vCenter Server 7.0 Update 1, you get prompts to provide vCenter Single Sign-On administrator password.

Workaround: If you run the update by using the vCenter Server Management Interface, you must provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in an interactive manner, you must interactively provide the vCenter Single Sign-On administrator password.

If you run the update by using software-packages or CLI in a non-interactive manner, you must provide the vCenter Single Sign-On administrator password by an answer file in the format

```
{ "vmdir.password": "SSO Password of Administrator@<SSO-DOMAIN> user" }
```

Smart Card and RSA SecurID authentication might stop working after upgrading to vCenter Server 7.0

If you have configured vCenter Server for either Smart Card or RSA SecurID authentication, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057 before starting the vSphere 7.0 upgrade process. If you do not perform the workaround as described in the KB, you might see the following error messages and Smart Card or RSA SecurID authentication does not work.

"Smart card authentication may stop working. Smart card settings may not be preserved, and smart card authentication may stop working."

or

"RSA SecurID authentication may stop working. RSA SecurID settings may not be preserved, and RSA SecurID authentication may stop working."

Workaround: Before upgrading to vSphere 7.0, see the VMware knowledge base article at https://kb.vmware.com/s/article/78057.

You might not be able to apply or remove NSX while you add ESXi hosts by using a vSphere Lifecycle Manager image to a cluster with enabled VMware vSphere High Availability

If you start an operation to apply or remove NSX while adding multiple ESXi hosts by using a vSphere Lifecycle Manager image to a vSphere HA-enabled cluster, the NSX-related operations might fail with an error in the vSphere Client such as:

```
vSphere HA agent on some of the hosts on cluster <cluster_name> is neither vSphere HA master agent nor connected to vSphere HA master agent. Verify that the HA configuration is correct.
```

The issue occurs because vSphere Lifecycle Manager configures vSphere HA for the ESXi hosts being added to the cluster one at a time. If you run an operation to apply or remove NSX while vSphere HA configure operations are still in progress, NSX operations might queue up between the vSphere HA configure operations for two different ESXi hosts. In such a case, the NSX operation fails with a cluster health check error, because the state of the cluster at that point does

not match the expected state that all ESXi hosts have vSphere HA configured and running. The more ESXi hosts you add to a cluster at the same time, the more likely the issue is to occur.

Workaround: Deactivate and enable Sphere HA on the cluster. Proceed with the operations to apply or remove NSX.

After an upgrade of a vCenter Server 7.0 system, you cannot see the IP addresses of pods in the vSphere Pod Summary tab of the vSphere Client

If you upgrade your vCenter Server 7.0 system to a later version, you can no longer see the IP addresses of pods in the **vSphere Pod Summary** tab of the vSphere Client.

Workaround: Use the Kubernetes CLI Tools for vSphere to review details of pods:

1. As a prerequisite, copy the pod and namespace names.
   - In the vSphere Client, navigate to **Workload Management** > **Clusters.**
   - Copy the IP displayed in the **Control Plane Node IP Address** tab.
   - You can navigate to `https://<control_plane_node_IP_address>` and download the Kubernetes CLI Tools, `kubectl` and `kubectl-vsphere`.
     Alternatively, follow the steps in Download and Install the Kubernetes CLI Tools for vSphere.
2. Use the CLI plug-in for vSphere to review the pod details.
   a. Log in to the Supervisor cluster by using the command
      `kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user account name> --insecure-skip-tls-verify`
   b. By using the names copied in step 1, run the commands for retrieving the pod details:
      `kubectl config use-context <namespace_name>`
      and
      `kubectl describe pod <pod_name> -n <namespace_name>`

As a result, you can see the IP address in an output similar to:

```
$ kubectl describe pod helloworld -n my-podvm-ns ...

Status: Running

IP: 10.0.0.10

IPs:

IP: 10.0.0.10 ...
```

Upgrading a vCenter Server with an external Platform Services Controller from 6.7u3 to 7.0 fails with VMAFD error

When you upgrade a vCenter Server deployment using an external Platform Services Controller, you converge the Platform Services Controller into a vCenter Server appliance. If the upgrade fails with the error `install.vmafd.vmdir_vdcpromo_error_21`, the VMAFD firstboot process has failed. The VMAFD firstboot process copies the VMware Directory Service Database (data.mdb) from the source Platform Services Controller and replication partner vCenter Server appliance.

Workaround: Deactivate TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) on the Ethernet adapter of the source Platform Services Controller or replication partner vCenter Server appliance before upgrading a vCenter Server with an external Platform Services Controller. See Knowledge Base article: https://kb.vmware.com/s/article/74678

vCenter Server system upgrades fail in the pre-check stage

Upgrades of your vCenter Server system might fail in the pre-check stage due to a limit in the authorization (Authz) connections. In the `/var/log/vmware/vpxd-svcs/vpxd-svcs*.log` file you see entries such as:

`Session count for user [after add]: <DOMAIN-NAME>\machine-xxxx is 200Session limit reached for user: <DOMAIN-NAME>\machine-xxxx with 200 sessions.`

You might also see delayed response from the vSphere Client to load the inventory.

Workaround: Restart vmware-vpxd-svcs in your vCenter Server system by using the command `service-control --restart vmware-vpxd-svcs` . Use the command only when no other activity runs in the vCenter Server system to avoid any interruptions to the workflow. For more information, see VMware knowledge base article 81953.

Upgrading vCenter Server using the CLI incorrectly preserves the Transport Security Layer (TLS) configuration for the vSphere Authentication Proxy service

If the vSphere Authentication Proxy service (`vmcam`) is configured to use a particular TLS protocol other than the default TLS 1.2 protocol, this configuration is preserved during the CLI upgrade process. By default, vSphere supports the TLS 1.2 encryption protocol. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS Configurator Utility to enable or deactivate different TLS protocol versions.

Workaround: Use the TLS Configurator Utility to configure the `vmcam` port. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3c by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from an vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle..`

However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3c fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3c or higher, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Smart card and RSA SecurID settings may not be preserved during vCenter Server upgrade

Authentication using RSA SecurID will not work after upgrading to vCenter Server 7.0. An error message will alert you to this issue when attempting to login using your RSA SecurID login.

Workaround: Reconfigure the smart card or RSA SecureID.

Upgrade to vSphere 7.0 Update 3c might require additional steps to force a full host-sync

The supported upgrade sequence for vSphere systems is first to upgrade vCenter Server and then ESXi. However, in certain environments with ESXi hosts of version 7.0 Update 2c and later, you need to update ESXi first to 7.0 Update 3c and then vCenter Server. Such an upgrade sequence requires additional steps to force a full host-sync.

Workaround: Log in to the appliance shell as a user with super administrative privileges (for example, `root`) and follow these steps:

1. Stop the vpxd service.
2. Run the command `/opt/vmware/vpostgres/current/bin/psql -U postgres -d VCDB -c "update VPX_HOST_SYNC_GEN set master_gen=0 where host_id in (select id from VPX_HOST where product_version like '7.0.3%')"`.
3. Start the vpxd service.

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with network error message

Migration of vCenter Server for Windows to vCenter Server appliance 7.0 fails with the error message `IP already exists in the network.` This prevents the migration process from configuring the network parameters on the new vCenter Server appliance. For more information, examine the log file: `/var/log/vmware/upgrade/UpgradeRunner.log`

Workaround:

1. Verify that all Windows Updates have been completed on the source vCenter Server for Windows instance, or deactivate automatic Windows Updates until after the migration finishes.
2. Retry the migration of vCenter Server for Windows to vCenter Server appliance 7.0.

Hot-patched ESXi hosts with both i40en and i40enu Intel network drivers installed might fail to configure vSphere High Availability after upgrade to vCenter Server 7.0 Update 3c

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3c adds an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. However, if you apply an ESXi hot patch that is released after vCenter Server 7.0 Update 3c and then upgrade your system to vCenter Server 7.0 Update 3c, the hot patch might not be listed in the precheck. As a result, you might not follow the proper steps to the upgrade and vSphere HA might fail to configure on such hosts.

Workaround: Upgrade the hot-patched ESXi hosts to version 7.0 Update 3c.

When you configure the number of virtual functions for an SR-IOV device by using the max_vfs module parameter, the changes might not take effect

In vSphere 7.0, you can configure the number of virtual functions for an SR-IOV device by using the Virtual Infrastructure Management (VIM) API, for example, through the vSphere Client. The task does not require reboot of the ESXi host. After you use the VIM API configuration, if you try to configure the number of SR-IOV virtual functions by using the `max_vfs` module parameter, the changes might not take effect because they are overridden by the VIM API configuration.

Workaround: None. To configure the number of virtual functions for an SR-IOV device, use the same method every time. Use the VIM API or use the `max_vfs` module parameter and reboot the ESXi host.

Upgraded vCenter Server appliance instance does not retain all the secondary networks (NICs) from the source instance

During a major upgrade, if the source instance of the vCenter Server appliance is configured with multiple secondary networks other than the VCHA NIC, the target vCenter Server instance will not retain secondary networks other than the VCHA NIC. If the source instance is configured with multiple NICs that are part of VDS port groups, the NIC configuration will not be preserved during the upgrade. Configurations for vCenter Server appliance instances that are part of the standard port group will be preserved.

Workaround: None. Manually configure the secondary network in the target vCenter Server appliance instance.

After upgrading or migrating a vCenter Server with an external Platform Services Controller, users authenticating using Active Directory lose access to the newly upgraded vCenter Server instance

After upgrading or migrating a vCenter Server with an external Platform Services Controller, if the newly upgraded vCenter Server is not joined to an Active Directory domain, users authenticating using Active Directory will lose access to the vCenter Server instance.

Workaround: Verify that the new vCenter Server instance has been joined to an Active Directory domain. See Knowledge Base article: https://kb.vmware.com/s/article/2118543

Migrating a vCenter Server for Windows with an external Platform Services Controller using an Oracle database fails

If there are non-ASCII strings in the Oracle events and tasks table the migration can fail when exporting events and tasks data. The following error message is provided: UnicodeDecodeError

Workaround: None.

After an ESXi host upgrade, a Host Profile compliance check shows non-compliant status while host remediation tasks fail

The non-compliant status indicates an inconsistency between the profile and the host.

This inconsistency might occur because ESXi 7.0 does not allow duplicate claim rules, but the profile you use contains duplicate rules. For example, if you attempt to use the Host Profile that you extracted from the host before upgrading ESXi 6.5 or ESXi 6.7 to version 7.0 and the Host Profile contains any duplicate claim rules of system default rules, you might experience the problems.

Workaround:

1. Remove any duplicate claim rules of the system default rules from the Host Profile document.
2. Check the compliance status.
3. Remediate the host.
4. If the previous steps do not help, reboot the host.

Error message displays in the vCenter Server Management Interface

After installing or upgrading to vCenter Server 7.0, when you navigate to the Update panel within the vCenter Server Management Interface, the error message "Check the URL and try again" displays. The error message does not prevent you from using the functions within the Update panel, and you can view, stage, and install any available updates.

Workaround: None.

Patching witness or passive nodes of environments with VMware vCenter Server High Availability enabled might fail

In environments with vCenter Server High Availability enabled, patching a witness or passive node might fail with a message similar to:

```
RuntimeError: unidentifiable C++ exception.
```

Workaround: Deactivate vCenter Server High Availability. Apply patches to your vCenter Server system. Re-enable vCenter Server High Availability.

After patching your vCenter Server system to vCenter Server 7.0.0a, the TLS version of the VC Storage Clients might revert to the default

If you have a TLS configuration for the VC Storage Clients service different from the default TLS 1.2 only, the TLS version might revert to the default after patching your vCenter Server system to vCenter Server 7.0.0a.

Workaround: Use the TLS Configuration utility to enable or deactivate TLS versions on your vCenter Server system after the update.

After updating your system to vCenter Server 7.0.0b, you see systemd core dump in the /var/core folder

After updating your system to vCenter Server 7.0.0b from either vCenter Server 7.0.0a or vCenter Server 7.0, in the `/var/core` folder you see systemd core dump, such as `core.systemd-journal.393` and `core.systemd-udevd.405`. The core dump is harmless and can be removed.

Workaround: None

After updating your vCenter Server system to 7.0.0b, the vCenter Server version is not updated in the Direct Console User Interface (DCUI)

After updating your system to vCenter Server 7.0.0b from vCenter Server 7.0.0a or vCenter Server 7.0, you still see the previous vCenter Server version in the DCUI.

Workaround: After you complete the update, to refresh the vCenter Server version, in the appliance shell, run the command `/usr/lib/applmgmt/dcui/notify`.

Update Planner fails with error Configured repository is not accessible due to network connectivity or incorrect URL

If you use Update Planner, which is part of vSphere Lifecycle Manager used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Configured repository is not accessible due to network connectivity or incorrect URL. Verify the repository settings.
```

The issue occurs when you use a custom local repository, such as `https:///uploads/dpe/` or a DBC path, to store the extracted . If the custom repository for URL-based patching has an authentication policy, Update Planner might not be able to fetch the list of available updates.

Workaround: Configure the custom repository such that authentication is not needed to access the custom repository URL.

After upgrading to vCenter Server 7.0.0b, you see vSphere HA errors on vSphere Lifecycle Manager Image based clusters

After upgrading to vCenter Server 7.0.0b, on vSphere Lifecycle Manager Image based clusters that are configured with vSphere HA, you might see error messages about the vSphere HA configuration after logging in for the first time to the environment. In the vSphere Client, you see messages such as:

`Cannot complete the configuration of the vSphere HA agent on the host.` or

`Applying HA VIBs on the cluster encountered a failure.`

The issue occurs because exports of the image depot might take long and cause a timeout of the task. In the `/storage/log/vmware/vmware-updatemgr/vum-server/vmware-vum-server.log` you see this message: `Export taking too long (Failure case)`

Workaround: This is a transient issue that resolves in 10 minutes after the vCenter Server is up and running. The issue does not affect any functionality. vSphere HA on the affected clusters operates as expected. All operations related to virtual machines, such as power on and migration, work across the vSphere HA-enabled clusters while this error recovery is still in progress.

You do not see a precheck error when patching to vCenter Server 7.0 Update 3d by using CLI

Due to the name change in the Intel i40en driver to i40enu and back to i40en, vCenter Server 7.0 Update 3d and later add an upgrade precheck to make sure that ESXi hosts affected from the change are properly upgraded. In some cases, if such hosts exist in your system, patching from a vCenter Server version earlier than 7.0 Update 3 to a version later than 7.0 Update 3 by using CLI might fail with the error `Installation failed. Retry to resume from the current state. Or please collect the VC support bundle.` . However, instead of this error, you must see the precheck error message.

Workaround: If you do not see the precheck error and patching your system to vCenter Server 7.0 Update 3d fails, make sure all ESXi hosts are upgraded to ESXi 7.0 Update 3d, by using either a baseline created from an ISO or a single image, before upgrading vCenter Server. Do not use patch baselines based on the rollup bulletin. You can find additional debug log information at `/var/log/vmware/applmgmt` . For more details, see VMware knowledge base articles 87319 and 86447.

Security Features Issues

Encrypted virtual machine fails to power on when HA-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled HA on the Trusted Cluster and one or more hosts in the cluster fails attestation, an encrypted virtual machine cannot power on.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Encrypted virtual machine fails to power on when DRS-enabled Trusted Cluster contains an unattested host

In VMware® vSphere Trust Authority™, if you have enabled DRS on the Trusted Cluster and one or more hosts in the cluster fails attestation, DRS might try to power on an encrypted virtual machine on an unattested host in the cluster. This operation puts the virtual machine in a locked state.

Workaround: Either remove or remediate all hosts that failed attestation from the Trusted Cluster.

Migrating or cloning encrypted virtual machines across vCenter Server instances fails when attempting to do so using the vSphere Client

If you try to migrate or clone an encrypted virtual machine across vCenter Server instances using the vSphere Client, the operation fails with the following error message: "The operation is not allowed in the current state."

Workaround: You must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances.

Networking Issues

When you use the VMware Remote Console, the envoy service might intermittently fail

An issue with the envoy service specific to the VMware Remote Console might lead to intermittent failures of the service. As a result, the vCenter Server Management Interface or vCenter Server APIs might also become unavailable.

Workaround: Use the vSphere Client as an alternative to the VMware Remote Console.

Reduced throughput in networking performance on Intel 82599/X540/X550 NICs

The new queue-pair feature added to ixgben driver to improve networking performance on Intel 82599EB/X540/X550 series NICs might reduce throughput under some workloads in vSphere 7.0 as compared to vSphere 6.7.

Workaround: To achieve the same networking performance as vSphere 6.7, you can deactivate the queue-pair with a module parameter. To deactivate the queue-pair, run the command:

```
# esxcli system module parameters set -p "QPair=0,0,0,0..." -m ixgben
```

After running the command, reboot.

If you try to deactivate vSphere with Tanzu on a vSphere cluster, the operation stops with an error

If some virtual machines outside of a Supervisor Cluster reside on any of the NSX segment port groups on the cluster, the cleanup script cannot delete such ports and deactivate vSphere with Tanzu on the cluster. In the vSphere Client, you see the error `Cleanup requests to NSX Manager failed` and the operation stops at `Removing` status. In the `/var/log/vmware/wcp/wcpsvc.log` file, you see an error message such as

```
Segment path=[...] has x VMs or VIFs attached. Disconnect all VMs and VIFs before deleting a segment.
```

Workaround: Delete the virtual machines indicated in the `/var/log/vmware/wcp/wcpsvc.log` file from the segment. Wait for the operation to restore.

After upgrading to NSX 6.4.7, when a static IPv6 address is assigned to workload VMs on an IPv6 network, the VMs are unable to ping the IPv6 gateway interface of the edge

This issue occurs after upgrading the vSphere Distributed Switches from 6.x to 7.0.

Workaround 1:

Select the VDS where all the hosts are connected, go to the **Edit** setting, and under **Multicast** option switch to basic.

Workaround 2:

Add the following rules on the edge firewall:

Ping allow rule.

Multicast Listener Discover (MLD) allow rule, which are icmp6, type 130 (v1) and type 143 (v2).

High throughput virtual machines may experience degradation in network performance when Network I/O Control (NetIOC) is enabled

Virtual machines requiring high network throughput can experience throughput degradation when upgrading from vSphere 6.7 to vSphere 7.0 with NetIOC enabled.

Workaround: Adjust the `ethernetx.ctxPerDev` setting to enable multiple worlds.

IPv6 traffic fails to pass through VMkernel ports using IPsec

When you migrate VMkernel ports from one port group to another, IPv6 traffic does not pass through VMkernel ports using IPsec.

Workaround: Remove the IPsec security association (SA) from the affected server, and then reapply the SA. To learn how to set and remove an IPsec SA, see the *vSphere Security* documentation.

Higher ESX network performance with a portion of CPU usage increase

ESX network performance may increase with a portion of CPU usage.

Workaround: Remove and add the network interface with only 1 rx dispatch queue. For example:

```
esxcli network ip interface remove --interface-name=vmk1
esxcli network ip interface add --interface-name=vmk1 --num-rxqueue=1
```

VM might lose Ethernet traffic after hot-add, hot-remove or storage vMotion

A VM might stop receiving Ethernet traffic after a hot-add, hot-remove or storage vMotion. This issue affects VMs where the uplink of the VNIC has SR-IOV enabled. PVRDMA virtual NIC exhibits this issue when the uplink of the virtual network is a Mellanox RDMA capable NIC and RDMA namespaces are configured.

Workaround: You can hot-remove and hot-add the affected Ethernet NICs of the VM to restore traffic. On Linux guest operating systems, restarting the network might also resolve the issue. If these workarounds have no effect, you can reboot the VM to restore network connectivity.

Change of IP address for a VCSA deployed with static IP address requires that you create the DNS records in advance

With the introduction of the DDNS, the DNS record update only works for VCSA deployed with DHCP configured networking. While changing the IP address of the vCenter server via VAMI, the following error is displayed:

The specified IP address does not resolve to the specified hostname.

Workaround: There are two possible workarounds.

1. Create an additional DNS entry with the same FQDN and desired IP address. Log in to the VAMI and follow the steps to change the IP address.

2. Log in to the VCSA using ssh. Execute the following script:
   `./opt/vmware/share/vami/vami_config_net`
   Use option 6 to change the IP adddress of eth0. Once changed, execute the following script:
   `./opt/likewise/bin/lw-update-dns`
   Restart all the services on the VCSA to update the IP information on the DNS server.

It may take several seconds for the NSX Distributed Virtual Port Group (NSX DVPG) to be removed after deleting the corresponding logical switch in NSX Manager.

As the number of logical switches increases, it may take more time for the NSX DVPG in vCenter Server to be removed after deleting the corresponding logical switch in NSX Manager. In an environment with 12000 logical switches, it takes approximately 10 seconds for an NSX DVPG to be deleted from vCenter Server.

Workaround: None.

Hostd runs out of memory and fails if a large number of NSX Distributed Virtual port groups are created.

In vSphere 7.0, NSX Distributed Virtual port groups consume significantly larger amounts of memory than opaque networks. For this reason, NSX Distributed Virtual port groups can not support the same scale as an opaque network given the same amount of memory.

Workaround:To support the use of NSX Distributed Virtual port groups, increase the amount of memory in your ESXi hosts. If you verify that your system has adequate memory to support your VMs, you can directly increase the memory of `hostd` using the following command.

```
localcli --plugin-dir /usr/lib/vmware/esxcli/int/ sched group setmemconfig --group-path
host/vim/vmvisor/hostd --units mb --min 2048 --max 2048
```

Note that this will cause `hostd` to use memory normally reserved for your environment's VMs. This may have the affect of reducing the number of VMs your ESXi host can support.

DRS may incorrectly launch vMotion if the network reservation is configured on a VM

If the network reservation is configured on a VM, it is expected that DRS only migrates the VM to a host that meets the specified requirements. In a cluster with NSX transport nodes, if some of the transport nodes join the transport zone by NSX-T Virtual Distributed Switch (N-VDS), and others by vSphere Distributed Switch (VDS) 7.0, DRS may incorrectly launch vMotion. You might encounter this issue when:

- The VM connects to an NSX logical switch configured with a network reservation.
- Some transport nodes join transport zone using N-VDS, and others by VDS 7.0, or, transport nodes join the transport zone through different VDS 7.0 instances.

Workaround: Make all transport nodes join the transport zone by N-VDS or the same VDS 7.0 instance.

When adding a VMkernel NIC (vmknic) to an NSX portgroup, vCenter Server reports the error "Connecting VMKernel adapter to a NSX Portgroup on a Stateless host is not a supported operation. Please use Distributed Port Group instead."

- For stateless ESXi on Distributed Virtual Switch (VDS), the vmknic on a NSX port group is blocked. You must instead use a Distributed Port Group.
- For stateful ESXi on VDS, vmknic on NSX port group is supported, but vSAN may have an issue if it is using vmknic on a NSX port group.

Workaround: Use a Distributed Port Group on the same VDS.

Enabling SRIOV from vCenter for QLogic 4x10GE QL41164HFCU CNA might fail

If you navigate to the **Edit Settings** dialog for physical network adapters and attempt to enable SR-IOV, the operation might fail when using QLogic 4x10GE QL41164HFCU CNA. Attempting to enable SR-IOV might lead to a network outage of the ESXi host.

Workaround: Use the following command on the ESXi host to enable SRIOV:

```
esxcfg-module
```

Storage Issues

VMFS datastores are not mounted automatically after disk hot remove and hot insert on HPE Gen10 servers with SmartPQI controllers

When SATA disks on HPE Gen10 servers with SmartPQI controllers without expanders are hot removed and hot inserted back to a different disk bay of the same machine, or when multiple disks are hot removed and hot inserted back in a different order, sometimes a new local name is assigned to the disk. The VMFS datastore on that disk appears as a snapshot and will not be mounted back automatically because the device name has changed.

Workaround: None. SmartPQI controller does not support unordered hot remove and hot insert operations.

ESXi might terminate I/O to NVMeOF devices due to errors on all active paths

Occasionally, all active paths to NVMeOF device register I/O errors due to link issues or controller state. If the status of one of the paths changes to Dead, the High Performance Plug-in (HPP) might not select another path if it shows high volume of errors. As a result, the I/O fails.

Workaround: Deactivate the configuration option **/Misc/HppManageDegradedPaths** to unblock the I/O.

VOMA check on NVMe based VMFS datastores fails with error

VOMA check is not supported for NVMe based VMFS datastores and will fail with the error:

```
ERROR: Failed to reserve device. Function not implemented
```

Example:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/: <partition#>
Running VMFS Checker version 2.1 in check mode
Initializing LVM metadata, Basic Checks will be done

Checking for filesystem activity
Performing filesystem liveness check..|Scanning for VMFS-6 host activity (4096 bytes/HB, 1024 HBs).
ERROR: Failed to reserve device. Function not implemented
Aborting VMFS volume check
VOMA failed to check device : General Error
```

Workaround: None. If you need to analyse VMFS metadata, collect it using the `-l` option, and pass to VMware customer support. The command for collecting the dump is:

```
voma -l -f dump -d /vmfs/devices/disks/:<partition#>
```

Using the VM reconfigure API to attach an encrypted First Class Disk to an encrypted virtual machine might fail with error

If an FCD and a VM are encrypted with different crypto keys, your attempts to attach the encrypted FCD to the encrypted VM using the `VM reconfigure API` might fail with the error message:

```
Cannot decrypt disk because key or password is incorrect.
```

Workaround: Use the `attachDisk API` rather than the `VM reconfigure API` to attach an encrypted FCD to an encrypted VM.

ESXi host might get in non responding state if a non-head extent of its spanned VMFS datastore enters the Permanent Device Loss (PDL) state

This problem does not occur when a non-head extent of the spanned VMFS datastore fails along with the head extent. In this case, the entire datastore becomes inaccessible and no longer allows I/Os.

In contrast, when only a non-head extent fails, but the head extent remains accessible, the datastore heartbeat appears to be normal. And the I/Os between the host and the datastore continue. However, any I/Os that depend on the failed non-head extent start failing as well. Other I/O transactions might accumulate while waiting for the failing I/Os to resolve, and cause the host to enter the non responding state.

Workaround: Fix the PDL condition of the non-head extent to resolve this issue.

After recovering from APD or PDL conditions, VMFS datastore with enabled support for clustered virtual disks might remain inaccessible

You can encounter this problem only on datastores where the clustered virtual disk support is enabled. When the datastore recovers from an All Paths Down (APD) or Permanent Device Loss (PDL) condition, it remains inaccessible. The VMkernel log might show multiple `SCSI3 reservation conflict` messages similar to the following:

```
2020-02-18T07:41:10.273Z cpu22:1001391219)ScsiDeviceIO: vm 1001391219:
SCSIDeviceCmdCompleteCB:2972: Reservation conflict retries 544 for command 0x45ba814b8340
(op: 0x89) to device "naa.624a9370b97601e346f64ba900024d53"
```

The problem can occur because the ESXi host participating in the cluster loses SCSI reservations for the datastore and cannot always reacquire them automatically after the datastore recovers.

Workaround: Manually register the reservation using the following command:

```
vmkfstools -L registerkey /vmfs/devices/disks/<device name>
```

where the `<device name>` is the name of the device on which the datastore is created.

Virtual NVMe Controller is the default disk controller for Windows 10 guest operating systems

The Virtual NVMe Controller is the default disk controller for the following guest operating systems when using Hardware Version 15 or later:

Windows 10

Windows Server 2016

Windows Server 2019

Some features might not be available when using a Virtual NVMe Controller. For more information, see https://kb.vmware.com/s/article/2147714

Note: Some clients use the previous default of LSI Logic SAS. This includes ESXi host client and PowerCLI.

Workaround: If you need features not available on Virtual NVMe, switch to VMware Paravirtual SCSI (PVSCSI) or LSI Logic SAS. For information on using VMware Paravirtual SCSI (PVSCSI), see https://kb.vmware.com/s/article/1010398

After an ESXi host upgrade to vSphere 7.0, presence of duplicate core claim rules might cause unexpected behavior

Claim rules determine which multipathing plugin, such as NMP, HPP, and so on, owns paths to a particular storage device. ESXi 7.0 does not support duplicate claim rules. However, the ESXi 7.0 host does not alert you if you add duplicate rules

to the existing claim rules inherited through an upgrade from a legacy release. As a result of using duplicate rules, storage devices might be claimed by unintended plugins, which can cause unexpected outcome.

Workaround: Do not use duplicate core claim rules. Before adding a new claim rule, delete any existing matching claim rule.

A CNS query with the compliance status filter set might take unusually long time to complete

The CNS QueryVolume API enables you to obtain information about the CNS volumes, such as volume health and compliance status. When you check the compliance status of individual volumes, the results are obtained quickly. However, when you invoke the CNS QueryVolume API to check the compliance status of multiple volumes, several tens or hundreds, the query might perform slowly.

Workaround: Avoid using bulk queries. When you need to get compliance status, query one volume at a time or limit the number of volumes in the query API to 20 or fewer. While using the query, avoid running other CNS operations to get the best performance.

New Deleted CNS volumes might temporarily appear as existing in the CNS UI

After you delete an FCD disk that backs a CNS volume, the volume might still show up as existing in the CNS UI. However, your attempts to delete the volume fail. You might see an error message similar to the following:

```
The object or item referred to could not be found.
```

Workaround: The next full synchronization will resolve the inconsistency and correctly update the CNS UI.

New Under certain circumstances, while a CNS operation fails, the task status appears as successful in the vSphere Client

This might occur when, for example, you use an incompliant storage policy to create a CNS volume. The operation fails, while the vSphere Client shows the task status as successful.

Workaround: The successful task status in the vSphere Client does not guarantee that the CNS operation succeeded. To make sure the operation succeeded, verify its results.

New Unsuccessful delete operation for a CNS persistent volume might leave the volume undeleted on the vSphere datastore

This issue might occur when the CNS Delete API attempts to delete a persistent volume that is still attached to a pod. For example, when you delete the Kubernetes namespace where the pod runs. As a result, the volume gets cleared from CNS and the CNS query operation does not return the volume. However, the volume continues to reside on the datastore and cannot be deleted through the repeated CNS Delete API operations.

Workaround: None.

vCenter Server and vSphere Client Issues

Vendor providers go offline after a PNID change

When you change the vCenter IP address (PNID change), the registered vendor providers go offline.

Workaround: Re-register the vendor providers.

Cross vCenter migration of a virtual machine fails with an error

When you use cross vCenter vMotion to move a VM's storage and host to a different vCenter server instance, you might receive the error `The operation is not allowed in the current state.`

This error appears in the UI wizard after the Host Selection step and before the Datastore Selection step, in cases where the VM has an assigned storage policy containing host-based rules such as encryption or any other IO filter rule.

Workaround: Assign the VM and its disks to a storage policy without host-based rules. You might need to decrypt the VM if the source VM is encrypted. Then retry the cross vCenter vMotion action.

Storage Sensors information in Hardware Health tab shows incorrect values on vCenter UI, host UI, and MOB

When you navigate to **Host > Monitor > Hardware Health > Storage Sensors** on vCenter UI, the storage information displays either incorrect or unknown values. The same issue is observed on the host UI and the MOB path `"runtime.hardwareStatusInfo.storageStatusInfo"` as well.

Workaround: None.

vSphere UI host advanced settings shows the current product locker location as empty with an empty default

vSphere UI host advanced settings shows the current product locker location as empty with an empty default. This is inconsistent as the actual product location `symlink` is created and valid. This causes confusion to the user. The default cannot be corrected from UI.

Workaround: User can use the esxcli command on the host to correct the current product locker location default as below.

1. Remove the existing Product Locker Location setting with: "`esxcli system settings advanced remove -o ProductLockerLocation`"

2. Re-add the Product Locker Location setting with the appropriate default:

2.a. If the ESXi is a full installation, the default value is "`/locker/packages/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/locker/packages/vmtoolsRepo"`

2.b. If the ESXi is a PXEboot configuration such as autodeploy, the default value is: "`/vmtoolsRepo`" `export PRODUCT_LOCKER_DEFAULT="/vmtoolsRepo"`

Run the following command to automatically figure out the location: `export PRODUCT_LOCKER_DEFAULT=`readlink /productLocker``

Add the setting: `esxcli system settings advanced add -d "Path to VMware Tools repository" -o ProductLockerLocation -t string -s $PRODUCT_LOCKER_DEFAULT`

You can combine all the above steps in step 2 by issuing the single command:

```
esxcli system settings advanced add -d "Path to VMware Tools repository" -o
ProductLockerLocation -t string -s `readlink /productLocker`
```

Skyline Health page displays garbage characters

In the vSphere Client, when you navigate to vCenter Server or select an ESXi host in the vSphere Client navigator and click Monitor > Skyline Health, the page displays garbage characters in the following locales: Korean, Japanese, German and French.

Workaround: Switch to English locale.

Virtual Machine Management Issues

Enter Maintenance Mode task fails when you try to perform maintenance on ESXi hosts where instant clones reside

In some cases, when you try to put in maintenance mode the ESXi hosts where instant clones reside, the task might fail with a ManagedObjectNotFound error. The issue occurs because some virtual machine objects enqueued for evacuation might be deleted while in-flight.

This issue is resolved in this release.

You cannot add or modify an existing network adapter on a virtual machine

If you try to add or modify an existing network adapter on a virtual machine, the Reconfigure Virtual Machine task might fail with an error such as `Cannot complete operation due to concurrent modification by another operation` in the vSphere Client. In the `/var/log/hostd.log` file of the ESXi host where the virtual machine runs, you see logs such as:

```
2020-07-28T07:47:31.621Z verbose hostd[2102259] [Originator@6876 sub=Vigor.Vmsvc.vm:/vmfs/volumes/vsan:526bc94351cf8f42-41153841cab2f9d9/bad71f5f-d85e-a276-4cf6-246e965d7154/interop_l2vpn_vmotion_VM_1.vmx] NIC: connection control message: Failed to connect virtual device 'ethernet0'.
```

In the `vpxa.log` file, you see entries similar to: `2020-07-28T07:47:31.941Z info vpxa[2101759] [Originator@6876 sub=Default opID=opId-59f15-19829-91-01-ed] [VpxLRO] -- ERROR task-138 -- vm-13 -- vim.VirtualMachine.reconfigure: vim.fault.GenericVmConfigFault:`

Workaround: For each ESXi host in your cluster do the following:

1. Connect to the ESXi host by using SSH and run the command
   `esxcli system module parameters set -a -p dvfiltersMaxFilters=8192 -m dvfilter`
2. Put the ESXi host in Maintenance Mode.
3. Reboot the ESXi host.

For more information, see VMware knowledge base article 80399.

ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors cannot join Enhanced vMotion Compatibility (EVC) AMD REV E or AMD REV F clusters on a vCenter Server 7.0 Update 1 system

In vCenter Server 7.0 Update 1, vSphere cluster services, such as vSphere DRS and vSphere HA, run on ESX agent virtual machines to make the services functionally independent of vCenter Server. However, the CPU baseline for AMD processors of the ESX agent virtual machines have POPCNT SSE4A instructions, which prevents ESXi 6.5 hosts with AMD Opteron Generation 3 (Greyhound) processors to enable EVC mode AMD REV E and AMD REV F on a vCenter Server 7.0 Update 1 system.

Workaround: None

The postcustomization section of the customization script runs before the guest customization

When you run the guest customization script for a Linux guest operating system, the `precustomization` section of the customization script that is defined in the customization specification runs before the guest customization and the `postcustomization` section runs after that. If you enable Cloud-Init in the guest operating system of a virtual machine, the `postcustomization` section runs before the customization due to a known issue in Cloud-Init.

Workaround: Deactivate Cloud-Init and use the standard guest customization.

Group migration operations in vSphere vMotion, Storage vMotion, and vMotion without shared storage fail with error

When you perform group migration operations on VMs with multiple disks and multi-level snapshots, the operations might fail with the error `com.vmware.vc.GenericVmConfigFault Failed waiting for data. Error 195887167. Connection closed by remote host, possibly due to timeout.`

Workaround: Retry the migration operation on the failed VMs one at a time.

Deploying an OVF or OVA template from a URL fails with a 403 Forbidden error

The URLs that contain an HTTP query parameter are not supported. For example, `http://webaddress.com?file=abc.ovf` or the Amazon pre-signed S3 URLs.

Workaround: Download the files and deploy them from your local file system.

Importing or deploying local OVF files containing non-ASCII characters in their name might fail with an error

When you import local `.ovf` files containing non-ASCII characters in their name, you might receive `400 Bad Request Error` . When you use such `.ovf` files to deploy a virtual machine in the vSphere Client, the deployment process stops at 0%. As a result, you might receive `400 Bad Request Error` or `500 Internal Server Error.`

Workaround:

1. Remove the non-ASCII characters from the `.ovf` and `.vmdk` file names.
   – To edit the `.ovf` file, open it with a text editor.
   – Search the non-ASCII `.vmdk` file name and change it to ASCII.
2. Import or deploy the saved files again.

New The third level of nested objects in a virtual machine folder is not visible

Perform the following steps:

1. Navigate to a data center and create a virtual machine folder.
2. In the virtual machine folder, create a nested virtual machine folder.
3. In the second folder, create another nested virtual machine, virtual machine folder, vApp, or VM Template.

As a result, from the VMs and Templates inventory tree you cannot see the objects in the third nested folder.

Workaround: To see the objects in the third nested folder, navigate to the second nested folder and select the VMs tab.

vSAN file services operations fail on vSphere Lifecycle Manager-enabled clusters

During a change in the state of an ESXi host, vSAN file services operations might fail on vSphere Lifecycle Manager-enabled clusters due to a race condition with the vSphere ESX Agent Manager (EAM). The problem happens during upgrades and operations, such as power on or power off, booting, or when the host exits maintenance or standby mode. The race condition occurs when an endpoint has been unavailable before the change of state of the ESXi host. In such cases, the EAM starts a remediation process that cannot be resolved and fails operations from other services, such as the vSAN file services.

Workaround: Restart the vSphere ESX Agent Manager.

vSphere HA and Fault Tolerance Issues

VMs in a cluster might be orphaned after recovering from storage inaccessibility such as a cluster wide APD

Some VMs might be in orphaned state after cluster wide APD recovers, even if HA and VMCP are enabled on the cluster.

This issue might be encountered when the following conditions occur simultaneously:

- All hosts in the cluster experience APD and do not recover until VMCP timeout is reached.
- HA primary initiates failover due to APD on a host.
- Power on API during HA failover fails due to one of the following:
  – APD across the same host
  – Cascading APD across the entire cluster
  – Storage issues
  – Resource unavailability
- FDM unregistration and VCs steal VM logic might initiate during a window where FDM has not unregistered the failed VM and VC's host synchronization responds that multiple hosts are reporting the same VM. Both FDM and VC unregister the different registered copies of the same VM from different hosts, causing the VM to be orphaned.

Workaround: You must unregister and reregister the orphaned VMs manually within the cluster after the APD recovers.

If you do not manually reregister the orphaned VMs, HA attempts failover of the orphaned VMs, but it might take between 5 to 10 hours depending on when APD recovers.

The overall functionality of the cluster is not affected in these cases and HA will continue to protect the VMs. This is an anomaly in what gets displayed on VC for the duration of the problem.

vSphere Lifecycle Manager Issues

You cannot enable NSX-T on a cluster that is already enabled for managing image setup and updates on all hosts collectively

NSX-T is not compatible with the vSphere Lifecycle Manager functionality for image management. When you enable a cluster for image setup and updates on all hosts in the cluster collectively, you cannot enable NSX-T on that cluster. However, you can deploy NSX Edges to this cluster.

Workaround: Move the hosts to a new cluster that you can manage with baselines and enable NSX-T on that new cluster.

vSphere Lifecycle Manager and vSAN File Services cannot be simultaneously enabled on a vSAN cluster in vSphere 7.0 release

If vSphere Lifecycle Manager is enabled on a cluster, vSAN File Services cannot be enabled on the same cluster and vice versa. In order to enable vSphere Lifecycle Manager on a cluster, which has VSAN File Services enabled already, first deactivate vSAN File Services and retry the operation. Please note that if you transition to a cluster that is managed by a single image, vSphere Lifecycle Manager cannot be deactivated on that cluster.

Workaround: None.

When a hardware support manager is unavailable, vSphere High Availability (HA) functionality is impacted

If hardware support manager is unavailable for a cluster that you manage with a single image, where a firmware and drivers addon is selected and vSphere HA is enabled, the vSphere HA functionality is impacted. You may experience the following errors.

- Configuring vSphere HA on a cluster fails.
- Cannot complete the configuration of the vSphere HA agent on a host: `Applying HA VIBs on the cluster encountered a failure.`
- Remediating vSphere HA fails: `A general system error occurred: Failed to get Effective Component map.`
- Disabling vSphere HA fails: Delete Solution task failed. `A general system error occurred: Cannot find hardware support package from depot or hardware support manager.`

Workaround:

- If the hardware support manager is temporarily unavailable, perform the following steps.

1. Reconnect the hardware support manager to vCenter Server.
2. Select a cluster from the Hosts and Cluster menu.
3. Select the Configure tab.
4. Under Services, click vSphere Availability.
5. Re-enable vSphere HA.

- If the hardware support manager is permanently unavailable, perform the following steps.

1. Remove the hardware support manager and the hardware support package from the image specification
2. Re-enable vSphere HA.
3. Select a cluster from the Hosts and Cluster menu.

4. Select the Updates tab.
5. Click Edit .
6. Remove the firmware and drivers addon and click Save.
7. Select the Configure tab.
8. Under Services, click vSphere Availability.
9. Re-enable vSphere HA.

I/OFilter is not removed from a cluster after a remediation process in vSphere Lifecycle Manager

Removing I/OFilter from a cluster by remediating the cluster in vSphere Lifecycle Manager, fails with the following error message: `iofilter XXX already exists` . The iofilter remains listed as installed.

Workaround:

1. Call IOFilter API `UninstallIoFilter_Task` from the vCenter Server managed object (IoFilterManager).
2. Remediate the cluster in vSphere Lifecycle Manager.
3. Call IOFilter API `ResolveInstallationErrorsOnCluster_Task` from the vCenter Server managed object (IoFilterManager) to update the database.

While remediating a vSphere HA enabled cluster in vSphere Lifecycle Manager, disabling and re-enabling vSphere HA causes a vSphere HA error state

Disabling and re-enabling vSphere HA during remediation process of a cluster, may fail the remediation process due to vSphere HA health checks reporting that hosts don't have vSphere HA VIBs installed. You may see the following error message: `Setting desired image spec for cluster failed.`

Workaround: After the cluster remediation operation has finished, deactivate and re-enable vSphere HA for the cluster.

Checking for recommended images in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the recommendation generation task could take more than an hour to finish or may appear to hang. The completion time for the recommendation task depends on the number of devices configured on each host and the number of image candidates from the depot that vSphere Lifecycle Manager needs to process before obtaining a valid image to recommend.

Workaround: None.

Checking for hardware compatibility in vSphere Lifecycle Manager has slow performance in large clusters

In large clusters with more than 16 hosts, the validation report generation task could take up to 30 minutes to finish or may appear to hang. The completion time depends on the number of devices configured on each host and the number of hosts configured in the cluster.

Workaround: None

Incomplete error messages in non-English languages are displayed, when remediating a cluster in vSphere Lifecycle Manager

You can encounter incomplete error messages for localized languages in the vCenter Server user interface. The messages are displayed, after a cluster remediation process in vSphere Lifecycle Manager fails. For example, your can observe the following error message.

The error message in English language: `Virtual machine 'VMC on DELL EMC -FileServer' that runs on cluster 'Cluster-1' reported an issue which prevents entering maintenance mode: Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

The error message in French language: `La VM « VMC on DELL EMC -FileServer », située sur le cluster « {Cluster-1} », a signalé un problème empêchant le passage en mode de maintenance : Unable to access the virtual machine configuration: Unable to access file[local-0] VMC on Dell EMC - FileServer/VMC on Dell EMC - FileServer.vmx`

Workaround: None.

When you convert a cluster that uses baselines to a cluster that uses a single image, a warning is displayed that vSphere HA VIBs will be removed

Converting a vSphere HA enabled cluster that uses baselines to a cluster that uses a single image, may result a warning message displaying that `vmware-fdm` component will be removed.

Workaround: This message can be ignored. The conversion process installs the `vmware-fdm` component.

If vSphere Update Manager is configured to download patch updates from the Internet through a proxy server, after upgrade to vSphere 7.0 that converts Update Manager to vSphere Lifecycle Manager, downloading patches from VMware patch repository might fail

In earlier releases of vCenter Server you could configure independent proxy settings for vCenter Server and vSphere Update Manager. After an upgrade to vSphere 7.0, vSphere Update Manager service becomes part of the vSphere Lifecycle Manager service. For the vSphere Lifecycle Manager service, the proxy settings are configured from the vCenter Server appliance settings. If you had configured Update Manager to download patch updates from the Internet through a proxy server but the vCenter Server appliance had no proxy setting configuration, after a vCenter Server upgrade to version 7.0, the vSphere Lifecycle Manager fails to connect to the VMware depot and is unable to download patches or updates.

Workaround: Log in to the vCenter Server Appliance Management Interface, https://*vcenter-server-appliance-FQDN-or-IP-address*:5480, to configure proxy settings for the vCenter Server appliance and enable vSphere Lifecycle Manager to use proxy.

If you use a Java client to review remediation tasks, you cannot extract the results from the remediation operations

If you use a Java client to review remediation tasks, extracting the results might fail with a `ConstraintValidationException` error. The issue occurs when an ESXi host fails to enter maintenance mode during the remediation and gets a status SKIPPED, but at the same time wrongly gets an In Progress flag for the consecutive remediation operations. This causes the `ConstraintValidationException` error on the Java Clients and you cannot extract the result of the remediation operation.

Workaround: Fix the underlying issues that prevent ESXi hosts to enter Maintenance Mode and retry the remediation operation.

The general vSphere Lifecycle Manager depot and local depots in Remote Office and Branch Office (ROBO) deployments might not be in sync

ROBO clusters that have limited or no access to the Internet or limited connectivity to vCenter Server can download an image from a depot that is local for them instead of accessing the vSphere Lifecycle Manager depot in vCenter Server. However, vSphere Lifecycle Manager generates software recommendations in the form of pre-validated images only on a central level and a recommended image content might not be available at a depot override.

Workaround: If you decide to use a recommended image, make sure the content between depot overrides and the central depot are in sync.

Cluster remediation by using the vSphere Lifecycle Manager might fail on ESXi hosts with enabled lockdown mode

If a cluster has ESXi hosts with enabled lockdown mode, remediation operations by using the vSphere Lifecycle Manager might skip such hosts. In the log files, you see messages such as `Host scan task failed` and `com.vmware.vcIntegrity.lifecycle.EsxImage.UnknownError An unknown error occurred while performing the operation.`.

Workaround: Add the root user to the exception list for lockdown mode and retry the cluster remediation.

You cannot use an ESXi image with OEM content to create clusters by using vSphere Lifecycle Manager workflows after an update

When you update an ESXi image with OEM content, for example Dell ESXi 7.0 Update 2a to Dell ESXi 7.0 Update 3d, some reserved VIBs, such that are present in the VMware base image but overridden by async VIBs packaged by the OEM, might be deleted. The same issue might occur after updating your system by using a non-critical baseline and then update to a higher version by using an ESXi image with OEM content. For example, if you update to 7.0 Update 2 by using a non-critical baseline and then update to 7.0 Update 3 by using a Dell ESXi 7.0 Update 3 image, reserved VIBs might also be deleted. As a result, you cannot use ESXi hosts with the updated version to create a vSphere Lifecycle Manager cluster managed by a single image. The operation fails and in the backtrace, you see errors such as:

```
2021-11-24T09:42:49Z lifecycle: 2101166: HostSeeding:956 ERROR Extract depot failed:
('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231', 'Failed to add reserved
VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not found in the reserved
VIB cache storage')2021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:373 ERROR
Extract depot failed.021-11-24T09:42:50Z lifecycle: 2101166: imagemanagerctl:152 ERROR
[ReservedVibExtractError] ('VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231',
'Failed to add reserved VIB VMW_bootbank_bnxtroce_216.0.58.0-23vmw.703.0.0.18644231: not
found in the reserved VIB cache storage')
```

Workaround: Use interactive or scripted upgrade instead of vSphere Lifecycle Manager workflows.

After you upgrade to vCenter Server 7.0.0b, in the vSphere Lifecycle Manager home view in the vSphere Client, you do not see the Show only rollup updates toggle button

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the **Show only rollup updates** toggle button might not be visible after you upgrade to vCenter Server 7.0.0b.

Workaround: After an upgrade to vCenter Server 7.0.0b, restart the vSphere Client. For more information, see Start, Stop, and Restart Services.

The Show only rollup updates toggle button is always turned on when you open a tab in the vSphere Lifecycle Manager home view in the vSphere Client

In vCenter Server 7.0.0b, you can use the **Show only rollup updates** toggle button to filter and select patches that you want to include in a baseline when you use the vSphere Lifecycle Manager.

The button is available in the **Updates** tab on the **Lifecycle Manager** pane, **Menu** > **Lifecycle Manager**, which is the vSphere Lifecycle Manager home view in the vSphere Client. The button is also available in the **Select Patches Manually** page on the **Baselines** tab in the **Create Baseline** wizard, which opens when you select **New** > **Baseline**.

However, the toggle button appears always turned on when you navigate to either of the **Updates** tab or the **Select Patches Manually** page. Even if you turn off the button when navigating away from the tab or page, it appears still turned on the next time you open them.

Workaround: None

When you use the Update Planner, in the vSphere Client you might see Unexpected error occurred while fetching the updates

When you use Update Planner, which is part of vSphere Lifecycle Manager, used to facilitate vCenter Server updates, you might see the following error in the vSphere Client:

```
Unexpected error occurred while fetching the updates
```

The issue occurs when you use a custom HTTPS port that prevents you from running interoperability reports by using the vSphere Client.

Workaround: Manually invoke the API. For more details, see the vSphere Automation API.

Miscellaneous Issues

Cannot migrate container volume due to insufficient space

The Migrate volume dialog in vSphere Client considers the current size of container volumes and the free space available on the target datastores. If the free space of a datastore is less than the volume size, then you cannot select the datastore for migration. vSphere preserves the storage policy as it migrates the volume, but the file size of the volume might change depending on the destination datastore type and its supported features. The vSphere Client might show the datastore has insufficient space to perform the migration, even though enough space is available.

Workaround: None

The Guest Power API returns 500 Internal Server Error

The Guest Power API intermittently returns an HTTP 500 error. The issue occurs after a restart of the VPXD service.

This issue is resolved in this release.

When applying a host profile with version 6.5 to a ESXi host with version 7.0, the compliance check fails

Applying a host profile with version 6.5 to a ESXi host with version 7.0, results in Coredump file profile reported as not compliant with the host.

Workaround: There are two possible workarounds.

1. When you create a host profile with version 6.5, set an advanced configuration option VMkernel.Boot.autoCreateDumpFile to false on the ESXi host.
2. When you apply an existing host profile with version 6.5, add an advanced configuration option VMkernel.Boot.autoCreateDumpFile in the host profile, configure the option to a fixed policy, and set value to false.

The Actions drop-down menu does not contain any items when your browser is set to language different from English

When your browser is set to language different from English and you click the **Switch to New View** button from the virtual machine **Summary** tab of the vSphere Client inventory, the **Actions** drop-down menu in the **Guest OS** panel does not contain any items.

Workaround: Select the **Actions** drop-down menu on the top of the virtual machine page.

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit minor throughput degradation when Dynamic Receive Side Scaling (DYN_RSS) or Generic RSS (GEN_RSS) feature is turned on

Mellanox ConnectX-4 or ConnectX-5 native ESXi drivers might exhibit less than 5 percent throughput degradation when DYN_RSS and GEN_RSS feature is turned on, which is unlikely to impact normal workloads.

Workaround: You can deactivate DYN_RSS and GEN_RSS feature with the following commands:

```
# esxcli system module parameters set -m nmlx5_core -p "DYN_RSS=0 GEN_RSS=0"
```

```
# reboot
```

RDMA traffic between two VMs on the same host might fail in PVRDMA environment

In a vSphere 7.0 implementation of a PVRDMA environment, VMs pass traffic through the HCA for local communication if an HCA is present. However, loopback of RDMA traffic does not work on qedrntv driver. For instance, RDMA Queue Pairs running on VMs that are configured under same uplink port cannot communicate with each other.

In vSphere 6.7 and earlier, HCA was used for local RDMA traffic if SRQ was enabled. vSphere 7.0 uses HCA loopback with VMs using versions of PVRDMA that have SRQ enabled with a minimum of HW v14 using RoCE v2.

The current version of Marvell FastLinQ adapter firmware does not support loopback traffic between QPs of the same PF or port.

Workaround: Required support is being added in the out-of-box driver certified for vSphere 7.0. If you are using the inbox qedrntv driver, you must use a 3-host configuration and migrate VMs to the third host.

Unreliable Datagram traffic QP limitations in qedrntv driver

There are limitations with the Marvell FastLinQ qedrntv RoCE driver and Unreliable Datagram (UD) traffic. UD applications involving bulk traffic might fail with qedrntv driver. Additionally, UD QPs can only work with DMA Memory Regions (MR). Physical MRs or FRMR are not supported. Applications attempting to use physical MR or FRMR along with UD QP fail to pass traffic when used with qedrntv driver. Known examples of such test applications are `ibv_ud_pingpong` and `ib_send_bw`.

Standard RoCE and RoCEv2 use cases in a VMware ESXi environment such as iSER, NVMe-oF (RoCE) and PVRDMA are not impacted by this issue. Use cases for UD traffic are limited and this issue impacts a small set of applications requiring bulk UD traffic.

Marvell FastLinQ hardware does not support RDMA UD traffic offload. In order to meet the VMware PVRDMA requirement to support GSI QP, a restricted software only implementation of UD QP support was added to the qedrntv driver. The goal of the implementation is to provide support for control path GSI communication and is not a complete implementation of UD QP supporting bulk traffic and advanced features.

Since UD support is implemented in software, the implementation might not keep up with heavy traffic and packets might be dropped. This can result in failures with bulk UD traffic.

Workaround: Bulk UD QP traffic is not supported with qedrntv driver and there is no workaround at this time. VMware ESXi RDMA (RoCE) use cases like iSER, NVMe, RDMA and PVRDMA are unaffected by this issue.

Servers equipped with QLogic 578xx NIC might fail when frequently connecting or disconnecting iSCSI LUNs

If you trigger QLogic 578xx NIC iSCSI connection or disconnection frequently in a short time, the server might fail due to an issue with the qfle3 driver. This is caused by a known defect in the device's firmware.

Workaround: None.

ESXi might fail during driver unload or controller disconnect operation in Broadcom NVMe over FC environment

In Broadcom NVMe over FC environment, ESXi might fail during driver unload or controller disconnect operation and display an error message such as: `@BlueScreen: #PF Exception 14 in world 2098707:vmknvmeGener IP 0x4200225021cc addr 0x19`

Workaround: None.

ESXi does not display OEM firmware version number of i350/X550 NICs on some Dell servers

The inbox ixgben driver only recognizes firmware data version or signature for i350/X550 NICs. On some Dell servers the OEM firmware version number is programmed into the OEM package version region, and the inbox ixgben driver does not read this information. Only the 8-digit firmware signature is displayed.

Workaround: To display the OEM firmware version number, install async ixgben driver version 1.7.15 or later.

X710 or XL710 NICs might fail in ESXi

When you initiate certain destructive operations to X710 or XL710 NICs, such as resetting the NIC or manipulating VMKernel's internal device tree, the NIC hardware might read data from non-packet memory.

Workaround: Do not reset the NIC or manipulate vmkernel internal device state.

NVMe-oF does not guarantee persistent VMHBA name after system reboot

NVMe-oF is a new feature in vSphere 7.0. If your server has a USB storage installation that uses vmhba30+ and also has NVMe over RDMA configuration, the VMHBA name might change after a system reboot. This is because the VMHBA name assignment for NVMe over RDMA is different from PCIe devices. ESXi does not guarantee persistence.

Workaround: None.

Backup fails for vCenter database size of 300 GB or greater

If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: `Timeout! Failed to complete in 72000 seconds`

Workaround: None.

A restore of vCenter Server 7.0 which is upgraded from vCenter Server 6.x with External Platform Services Controller to vCenter Server 7.0 might fail

When you restore a vCenter Server 7.0 which is upgraded from 6.x with External Platform Services Controller to vCenter Server 7.0, the restore might fail and display the following error: `Failed to retrieve appliance storage list`

Workaround: During the first stage of the restore process, increase the storage level of the vCenter Server 7.0. For example if the vCenter Server 6.7 External Platform Services Controller setup storage type is small, select storage type large for the restore process.

Enabled SSL protocols configuration parameter is not configured during a host profile remediation process

`Enabled SSL protocols` configuration parameter is not configured during a host profile remediation and only the system default protocol `tlsv1.2` is enabled. This behavior is observed for a host profile with version 7.0 and earlier in a vCenter Server 7.0 environment.

Workaround: To enable TLSV 1.0 or TLSV 1.1 SSL protocols for SFCB, log in to an ESXi host by using SSH, and run the following ESXCLI command: `esxcli system wbem -P <protocol_name>`

Unable to configure Lockdown Mode settings by using Host Profiles

Lockdown Mode cannot be configured by using a security host profile and cannot be applied to multiple ESXi hosts at once. You must manually configure each host.

Workaround: In vCenter Server 7.0, you can configure Lockdown Mode and manage Lockdown Mode exception user list by using a security host profile.

When a host profile is applied to a cluster, Enhanced vMotion Compatibility (EVC) settings are missing from the ESXi hosts

Some settings in the VMware config file `/etc/vmware/config` are not managed by Host Profiles and are blocked, when the config file is modified. As a result, when the host profile is applied to a cluster, the EVC settings are lost, which causes loss of EVC functionalities. For example, unmasked CPUs can be exposed to workloads.

Workaround: Reconfigure the relevant EVC baseline on cluster to recover the EVC settings.

Using a host profile that defines a core dump partition in vCenter Server 7.0 results in an error

In vCenter Server 7.0, configuring and managing a core dump partition in a host profile is not available. Attempting to apply a host profile that defines a core dump partition, results in the following error: `No valid coredump partition found.`

Workaround: None. In vCenter Server 7.0., Host Profiles supports only file-based core dumps.

You cannot paste by right clicking in the vi editor

If you use the vi text editor on a vCenter Server Appliance instance, you cannot paste previously copied content by right clicking. Instead, the vi editor changes mode to Visual.

Workaround: From the vCenter Server Appliance shell, run the command`/usr/bin/sed -i.bak -E '2alet skip_defaults_vim=1' /etc/vimrc`.

HTTP requests from certain libraries to vSphere might be rejected

The HTTP reverse proxy in vSphere 7.0 enforces stricter standard compliance than in previous releases. This might expose pre-existing problems in some third-party libraries used by applications for SOAP calls to vSphere.

If you develop vSphere applications that use such libraries or include applications that rely on such libraries in your vSphere stack, you might experience connection issues when these libraries send HTTP requests to VMOMI. For example, HTTP requests issued from vijava libraries can take the following form:

```
POST /sdk HTTP/1.1
SOAPAction
Content-Type: text/xml; charset=utf-8
User-Agent: Java/1.8.0_221
```

The syntax in this example violates an HTTP protocol header field requirement that mandates a colon after SOAPAction. Hence, the request is rejected in flight.

Workaround: Developers leveraging noncompliant libraries in their applications can consider using a library that follows HTTP standards instead. For example, developers who use the vijava library can consider using the latest version of the yavijava library instead.

SNMP dynamic firewall ruleset is modified by Host Profiles during a remediation process

The SNMP firewall ruleset is a dynamic state, which is handled during runtime. When a host profile is applied, the configuration of the ruleset is managed simultaneously by Host Profiles and SNMP, which can modify the firewall settings unexpectedly.

Workaround: There are two possible workarounds.

- To allow the ruleset to manage itself dynamically, exclude the SNMP firewall ruleset option in the configuration of the host profile.
- To proceed with the double management of the ruleset, when needed, correct the firewall ruleset state.

You might see a dump file when using Broadcom driver lsi_msgpt3, lsi_msgpt35 and lsi_mr3

When using the lsi_msgpt3, lsi_msgpt35 and lsi_mr3 controllers, there is a potential risk to see dump file lsuv2-lsi-drivers-plugin-util-zdump. There is an issue when exiting the storelib used in this plugin utility. There is no impact on ESXi operations, you can ignore the dump file.

Workaround: You can safely ignore this message. You can remove the lsuv2-lsi-drivers-plugin with the following command:

```
esxcli software vib remove -n lsuv2-lsiv2-drivers-plugin
```

You might see reboot is not required after configuring SR-IOV of a PCI device in vCenter, but device configurations made by third party extensions might be lost and require reboot to be re-applied.

In ESXi 7.0, SR-IOV configuration is applied without a reboot and the device driver is reloaded. ESXi hosts might have third party extensions perform device configurations that need to run after the device driver is loaded during boot. A reboot is required for those third party extensions to re-apply the device configuration.

Workaround: You must reboot after configuring SR-IOV to apply third party device configurations.

You see black or grey zones in the background of a parent window in the Direct Console User Interface (DCUI) after a child window closes

In the DCUI, when you close a child window by pressing the ESC or Enter keys, or the **Cancel** or **OK** buttons, the parent window appearance might change. The background color changes to grey or black for some part of the parent window. However, all required information from the DCUI is properly displayed and all operations performed in the DCUI complete successfully.

Workaround: Wait for 1 minute without refreshing the current window in the DCUI or pressing any key.

Backup Issues

If you use the NFS and SMB protocols for file-based backup of vCenter Server, the backup fails after an update from vCenter Server 7.x to vCenter Server 7.0 Update 1

If you use the Network File System (NFS) and Server Message Block (SMB) protocols for file-based backup of vCenter Server, the backup fails after an update from an earlier version of vCenter Server 7.x to vCenter Server 7.0 Update 1. In the `applmgmt.log` , you see an error message such as `Failed to mount the remote storage` . The issue occurs because of Linux kernel updates that run during the patch process. The issue does not occur on fresh installations of vCenter Server 7.0 Update 1.

Workaround: Reboot the vCenter Server appliance after the update is complete.

Microsoft Active Directory Federation Services (ADFS) logins might fail after restoring a vCenter Server Appliance

If you manually add a certificate to the vCenter Server JRE truststore or modify the `/etc/hosts` file when setting up ADFS, the changes are not preserved after restoring and might cause ADFS logins to fail.

Workaround: Add the ADFS certificate to the vCenter Server JRE truststore after restoring your vCenter Server Appliance. For more information, see Import the Trusted Certificate of an External Identity Provider. Add the necessary host name mappings back to the `/etc/hosts` file after restoring your vCenter Server Appliance.

vCenter Release Notes Before Mar'23

Release notes published before March 2023 are available in pdf format:

VMware vSphere

VMware vSphere 7.0 Release Notes

VMware vCenter

VMware vCenter Server 7.0 Update 3l Release Notes

VMware vCenter Server 7.0 Update 3k Release Notes

VMware vCenter Server 7.0 Update 3j Release Notes

VMware vCenter Server 7.0 Update 3i Release Notes

VMware vCenter Server 7.0 Update 3h Release Notes

VMware vCenter Server 7.0 Update 3g Release Notes

VMware vCenter Server 7.0 Update 3f Release Notes

VMware vCenter Server 7.0 Update 3e Release Notes

VMware vCenter Server 7.0 Update 3d Release Notes

VMware vCenter Server 7.0 Update 3c Release Notes

VMware vCenter Server 7.0 Update 3a Release Notes

VMware vCenter Server 7.0 Update 3 Release Notes

VMware vCenter Server 7.0 Update 2d Release Notes

VMware vCenter Server 7.0 Update 2c Release Notes

VMware vCenter Server 7.0 Update 2b Release Notes

VMware vCenter Server 7.0 Update 2a Release Notes

VMware vCenter Server 7.0 Update 2 Release Notes

VMware vCenter Server 7.0 Update 1d Release Notes

VMware vCenter Server 7.0 Update 1c Release Notes

VMware vCenter Server 7.0 Update 1a Release Notes

VMware vCenter Server 7.0 Update 1 Release Notes

VMware vCenter Server 7.0.0d Release Notes

VMware vCenter Server 7.0.0c Release Notes

VMware vCenter Server 7.0.0b Release Notes

VMware vCenter Server 7.0.0a Release Notes

VMware Host Client Release Notes

VMware Host Client 1.37.0 Release Notes

This document contains the following sections

- Introduction
- What's in the Release Notes
- Resolved Issues
- Known Issues

Introduction

VMware Host Client 1.37.0 | 05 OCTOBER 2021 | 18255732
Check for additions and updates to these release notes.

What's in the Release Notes

- ESXi 7.0 Update 3 delivers bugs and security fixes documented in the Resolved Issues section.

The release notes cover the following topics:

VMware Host Client Overview

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts. It can be used to perform administrative tasks to manage host resources such as virtual machines, networking, and storage. The VMware Host Client can also be helpful for troubleshooting individual virtual machines or hosts if vCenter Server and the vSphere Client are unavailable.

For more information, see the vSphere 7.0 Documentation.

Previous Releases

- VMware Host Client 1.34.8
- VMware Host Client 1.34.4
- VMware Host Client 1.34.0
- VMware Host Client 1.33.3
- VMware Host Client 1.30.0
- VMware Host Client 1.25.0
- VMware Host Client 1.21
- VMware Host Client 1.8
- VMware Host Client 1.4
- VMware Host Client 1.2
- VMware Host Client 1.0

Resolved Issues

- **You cannot log in to VMware Host Client with Internet Explorer 11**
  When you try to log in to VMware Host Client with Internet Explorer 11, you might see the **Object Doesn't support property or method 'padstart'** error.
  This issue is resolved in this release.

Known Issues

- **Resizing the disk partitions in VMware Host Client UI might cause redundant partitions**
  When you hold down the left mouse button and move the slider back and forth several times, a redundant number of partitions appears in the UI.
  Workaround: Hold down the left mouse button for some time and than move the slider back and forth.
- **You cannot increase the LUN size of the VMFS datastore**
  When you try to increase the LUN size of the Fibre Channel storage, the operation might fail. The value field accepts only MB due to a problem with the horizontal scroller. The issue is not browser-specific.
  Workaround: Use Secure Shell (SSH) to increase the LUN size and then reboot the relevant host.
- **The welcome message does not appear on the VMware Host Client login page**
  When you try to log in to the VMware Host Client, the welcome message set through the configuration manager does not appear. You might encounter the problem if the message is updated through the VMware Host Client UI.
  Workaround: You must manually create the **welcome.txt** file in **/etc/vmware**. After each reboot of the ESXi host, recreate the **/etc/vmware/welcome** file in the same location.

VMware Host Client 1.34.8 Release Notes

This document contains the following sections

- Introduction
- What's in the Release Notes
- Resolved Issues
- Known Issues

Introduction

VMware Host Client 1.34.8 | 09 MARCH 2021 | 17417756
Check for additions and updates to these release notes.

What's in the Release Notes

- ESXi 7.0 Update 2 includes an updated version of the VMware Host Client with the following additional features:
  - Support for virtual machine hardware version 19

The release notes cover the following topics:

VMware Host Client Overview

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts. It can be used to perform administrative tasks to manage host resources such as virtual machines, networking, and storage. The VMware Host Client can also be helpful for troubleshooting individual virtual machines or hosts if vCenter Server and the vSphere Client are unavailable.

For more information, see the vSphere 7.0 Documentation.

Previous Releases

- VMware Host Client 1.34.4
- VMware Host Client 1.34.0
- VMware Host Client 1.33.3
- VMware Host Client 1.30.0
- VMware Host Client 1.25.0
- VMware Host Client 1.21
- VMware Host Client 1.8
- VMware Host Client 1.4
- VMware Host Client 1.2
- VMware Host Client 1.0

Resolved Issues

- **You cannot log in to VMware Host Client with Internet Explorer 11**
  When you try to log in to VMware Host Client with Internet Explorer 11, you might see the **Object Doesn't support property or method 'padstart'** error.
  This issue is resolved in this release.

Known Issues

- **Resizing the disk partitions in VMware Host Client UI might cause redundant partitions**
  When you hold down the left mouse button and move the slider back and forth several times, a redundant number of partitions appears in the UI.
  Workaround: Hold down the left mouse button for some time and than move the slider back and forth.

- **You cannot increase the LUN size of the VMFS datastore**
  When you try to increase the LUN size of the Fibre Channel storage, the operation might fail. The value field accepts only MB due to a problem with the horizontal scroller. The issue is not browser-specific.
  Workaround: Use Secure Shell (SSH) to increase the LUN size and then reboot the relevant host.
- **The welcome message does not appear on the VMware Host Client login page**
  When you try to log in to the VMware Host Client, the welcome message set through the configuration manager does not appear. You might encounter the problem if the message is updated through the VMware Host Client UI.
  Workaround: You must manually create the **welcome.txt** file in **/etc/vmware**. After each reboot of the ESXi host, recreate the **/etc/vmware/welcome** file in the same location.

VMware Host Client 1.34.4 Release Notes

This document contains the following sections

- Introduction
- What's in the Release Notes
- Known Issues

Introduction

VMware Host Client 1.34.4 | 06 OCTOBER 2020 | 16668064 Check for additions and updates to these release notes.

What's in the Release Notes

- ESXi 7.0 includes an updated version of the VMware Host Client with the following additional features:
  - Support for virtual machine hardware version 18
  - Support for virtual machine memory size up to 24 TB
  - Support for allocation of up to 768 virtual CPUs per virtual machine

The release notes cover the following topics:

VMware Host Client Overview

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts. It can be used to perform administrative tasks to manage host resources such as virtual machines, networking, and storage. The VMware Host Client can also be helpful for troubleshooting individual virtual machines or hosts if vCenter Server and the vSphere Client are unavailable.

For more information, see the vSphere 7.0 Documentation.

Previous Releases

- VMware Host Client 1.34.0
- VMware Host Client 1.33.3
- VMware Host Client 1.30.0
- VMware Host Client 1.25.0
- VMware Host Client 1.21
- VMware Host Client 1.8
- VMware Host Client 1.4
- VMware Host Client 1.2
- VMware Host Client 1.0

Known Issues

- **You cannot increase the LUN size of the VMFS datastore**
  When you try to increase the LUN size of the Fibre Channel storage, the operation might fail. The value field accepts only MB due to a problem with the horizontal scroller. The issue is not browser-specific.
  Workaround: Use Secure Shell (SSH) to increase the LUN size and then reboot the relevant host.
- **The welcome message does not appear on the VMware Host Client login page**
  When you try to log in to the VMware Host Client, the welcome message set through the configuration manager does not appear. You might encounter the problem if the message is updated through the VMware Host Client UI.
  Workaround: You must manually create the **welcome.txt** file in **/etc/vmware**. After each reboot of the ESXi host, recreate the **/etc/vmware/welcome** file in the same location.

VMware Host Client 1.34.0 Release Notes

This document contains the following sections

- Introduction
- What's in the Release Notes

Introduction

Updated on: 02 APRIL 2020
VMware Host Client 1.34.0 | 02 APRIL 2020 | 15603211
Check for additions and updates to these release notes.

What's in the Release Notes

- ESXi 7.0 includes an updated version of the VMware Host Client with the following additional features:
  - Support for virtual machine hardware versions 16 and 17
  - Support for Precision Time Protocol (PTP)
  - Support for the Intel Software Guard Extensions (SGX) technology
  - Ability to add new virtual machine devices such as the Watchdog Timer device, Precision Clock device, and Dynamic PCI device

The release notes cover the following topics:

VMware Host Client Overview

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts. It can be used to perform administrative tasks to manage host resources such as virtual machines, networking, and storage. The VMware Host Client can also be helpful for troubleshooting individual virtual machines or hosts if vCenter Server and the vSphere Client are unavailable.

For more information, see the vSphere 7.0 Documentation.

Previous Releases

- VMware Host Client 1.33.3
- VMware Host Client 1.30.0
- VMware Host Client 1.25.0
- VMware Host Client 1.21
- VMware Host Client 1.8
- VMware Host Client 1.4

- VMware Host Client 1.2
- VMware Host Client 1.0

ESXi Installation and Setup

VMware ESXi Installation and Setup describes how to install and configure VMware ESXi™.

In this guide:

- About VMware ESXi Installation and Setup
- Introduction to vSphere Installation and Setup
- Overview of the vSphere Installation and Setup Process
- About ESXi Evaluation and Licensed Modes
- Installing and Setting Up ESXi
- Troubleshooting ESXi Booting
- Decommission an ESXi Host

ESXi Installation and Setup

VMware ESXi Installation and Setup describes how to install and configure VMware ESXi™.

In this guide:

- About VMware ESXi Installation and Setup
- Introduction to vSphere Installation and Setup
- Overview of the vSphere Installation and Setup Process
- About ESXi Evaluation and Licensed Modes
- Installing and Setting Up ESXi
- Troubleshooting ESXi Booting
- Decommission an ESXi Host

About VMware ESXi Installation and Setup

VMware ESXi Installation and Setup describes how to install and configure VMware ESXi™.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we have updated this guide to remove instances of non-inclusive language.

Intended Audience

VMware ESXi Installation and Setup is intended for experienced administrators who want to install and configure ESXi.

This information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. The information about using the Image Builder and VMware vSphere®Auto Deploy™ is written for administrators who have experience with Microsoft PowerShell and VMware vSphere® PowerCLI™.

Introduction to vSphere Installation and Setup

vSphere 7.0 provides various options for installation and setup. To ensure a successful vSphere deployment, you should understand the installation and setup options, and the sequence of tasks.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. vCenter Server lets you pool and manage the resources of multiple hosts.

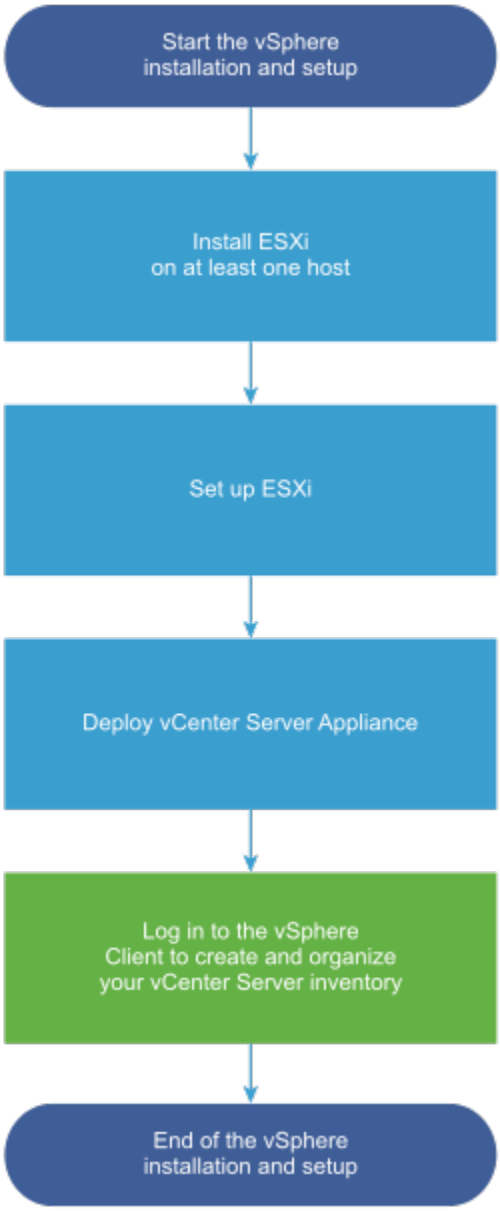
You deploy the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy the vCenter Server appliance on ESXi hosts or on vCenter Server instances.

Overview of the vSphere Installation and Setup Process

vSphere is a sophisticated product with multiple components to install and set up. To ensure a successful vSphere deployment, understand the sequence of tasks required.

Installing vSphere includes the following tasks:

Figure 1: vSphere Installation and Setup Workflow



1. Read the vSphere release notes.
2. Install ESXi.
3. Install vCenter Server.

About ESXi Evaluation and Licensed Modes

You can use evaluation mode to explore a set of features equal to the vSphere Enterprise Plus license.

You can use evaluation mode to explore the entire set of features for ESXi hosts. The evaluation mode provides the set of features equal to a vSphere Enterprise Plus license. Before the evaluation mode expires, you must assign to your hosts a license that supports all the features in use. For example, in evaluation mode, you can use vSphere vMotion technology, the vSphere HA feature, the vSphere DRS feature, and other features. If you want to continue using these features, you must assign a license that supports them.

The installable version of ESXi hosts is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal storage device by your hardware vendor. It might be in evaluation mode or prelicensed.

The evaluation period is 60 days and begins when you turn on the ESXi host. At any time during the 60-day evaluation period, you can convert from evaluation mode to licensed mode. The time available in the evaluation period is decreased by the time already used.

For example, suppose that you use an ESXi host in evaluation mode for 20 days and then assign a vSphere Standard Edition license key to the host. If you set the host back in evaluation mode, you can explore the entire set of features for the host for the remaining evaluation period of 40 days.

For ESXi hosts, license or evaluation period expiry leads to disconnection from vCenter Server. All powered on virtual machines continue to work, but you cannot power on virtual machines after they are powered off. You cannot change the current configuration of the features that are in use. You cannot use the features that remained unused before the license expiration.

For information about managing licensing for ESXi hosts, see the *vCenter Server and Host Management* documentation.

Installing and Setting Up ESXi

You can install and set up ESXi on your physical hardware so that it acts as a platform for virtual machines.

In this chapter:

- ESXi Requirements
- Preparing for Installing ESXi
- Installing ESXi
- Setting Up ESXi
- After You Install and Set Up ESXi

ESXi Requirements

To install or upgrade ESXi, your system must meet specific hardware and software requirements.

- ESXi System Storage Overview
- ESXi Hardware Requirements
- Supported Remote Management Server Models and Firmware Versions
- Recommendations for Enhanced ESXi Performance
- Incoming and Outgoing Firewall Ports for ESXi Hosts
- Required Free Space for System Logging
- VMware Host Client System Requirements
- ESXi Passwords and Account Lockout

ESXi System Storage Overview

ESXi7.0 introduces a system storage layout that allows flexible partition management and support for large modules, and third-party components, while facilitating debugging.

ESXi7.0 System Storage Changes

Before ESXi7.0 , partition sizes were fixed, except for the `/scratch` partition and the optional VMFS datastore, and the partition numbers were static, limiting partition management. With ESXi7.0, partitions are consolidated into fewer, larger partitions that are expandable, depending on the used boot media and its capacity.

The ESXi7.0 system storage layout consists of four partitions:

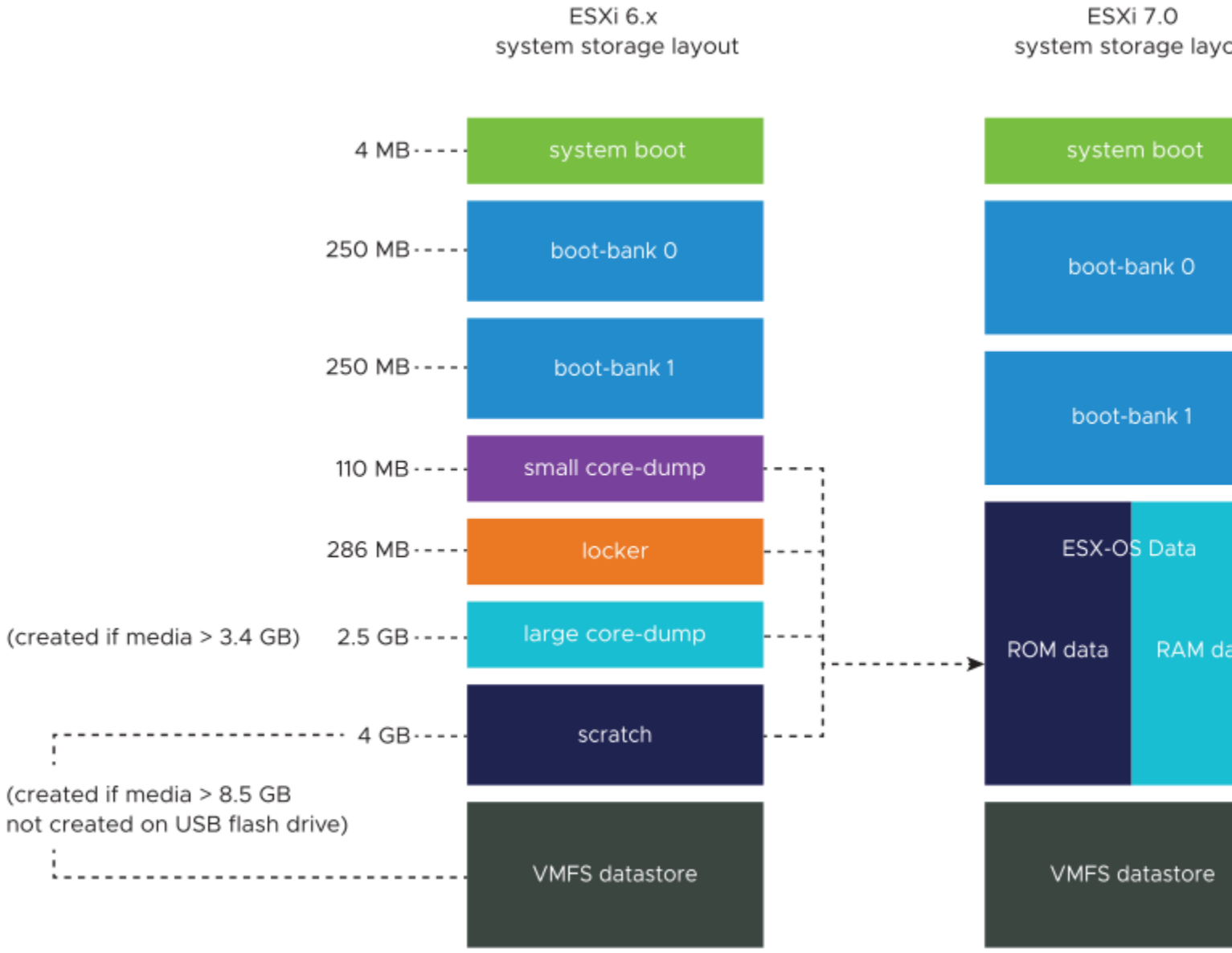
Table 1: ESXi 7.0 system storage partitions:

Partition	Use	Type
System Boot	Stores boot loader and EFI modules.	FAT16
Boot-bank 0	System space to store ESXi boot modules.	FAT16
Boot-bank 1	System space to store ESXi boot modules.	FAT16
ESX-OSData	Acts as the unified location to store additional modules. Not used for booting and virtual machines. Consolidates the legacy `/scratch` partition, locker partition for VMware Tools, and core dump destinations. **CAUTION:** Always create ESX-OSData partitions on persistent storage device that is not shared between ESXi hosts. Use USB, SD and non-USB flash media devices only for boot bank partitions.	VMFS-L

The ESX-OSData volume is divided into two high-level categories of data, persistent and non-persistent data. Persistent data contains of data written infrequently, for example, VMware Tools ISOs, configurations, and core dumps.

Non-persistent data contains of frequently written data, for example, logs, VMFS global traces, vSAN Entry Persistence Daemon (EPD) data, vSAN traces, and real-time databases.

Figure 2: Consolidated system storage in ESXi 7.0 and later



ESXi7.0 System Storage Sizes

Partition sizes, except for the system boot partition, can vary depending on the size of the boot media used. If the boot media is a high-endurance one with capacity larger than 142 GB, a VMFS datastore is created automatically to store virtual machine data.

You can review the boot media capacity and the automatic sizing as configured by the ESXi installer by using the vSphere Client and navigating to the **Partition Details** view. Alternatively, you can use ESXCLI, for example the `esxcli storage filesystem list` command.

Table 2: ESXi7.0 System Storage Sizes, Depending on the Used Boot Media and Its Capacity.

Boot Media Size	8-10 GB	10-32 GB	32-128 GB	>128 GB
System Boot	100 MB	100 MB	100 MB	100 MB
Boot-bank 0	500 MB	1 GB	4 GB	4 GB
Boot-bank 1	500 MB	1 GB	4 GB	4 GB
ESX-OSData	remaining space	remaining space	remaining space	up to 128 GB
VMFS datastore				remaining space for media size > 142 GB

Starting with vSphere 7.0 Update 1c, you can use the ESXi installer boot option `systemMediaSize` to limit the size of system storage partitions on the boot media. If your system has a small footprint that does not require the maximum of 128 GB of system storage size, you can limit it to the minimum of 32 GB. The `systemMediaSize` parameter accepts the following values:

- min (32 GB, for single disk or embedded servers)
- small (64 GB, for servers with at least 512 GB of RAM)
- default (128 GB)
- max (consume all available space, for multi-terabyte servers)

The selected value must fit the purpose of your system. For example, a system with 1 TB of memory must use the minimum of 64 GB for system storage. To set the boot option at install time, for example `systemMediaSize=small` , refer to Enter Boot Options to Start an Installation or Upgrade Script. For more information, see Knowledge Base article 81166.

ESXi7.0 System Storage Links

The sub-systems that require access to the ESXi partitions, access these partitions by using the following symbolic links:

Table 3: ESXi7.0 system storage symbolic links.

System Storage Volume	Symbolic Link
Boot-bank 0	`/bootbank`
Boot-bank 1	`/altbootbank`

Persistent data	`/productLocker`
	`/locker`
	`/var/core`
	`/usr/lib/vmware/isoimages`
	`/usr/lib/vmware/floppies`

Non-persistent data	`/var/run`
	`/var/log`
	`/var/vmware`
	`/var/tmp`
	`/scratch`

ESXi Hardware Requirements

Make sure that the host meets the minimum hardware configurations supported by ESXi7.0.

Hardware and System Resources

To install or upgrade ESXi, your hardware and system resources must meet the following requirements:

- Supported server platform. For a list of supported platforms, see the VMware Compatibility Guide.
- ESXi7.0 requires a host with at least two CPU cores.
- ESXi7.0 supports a broad range of multi-core of 64-bit x86 processors. For a complete list of supported processors, see the VMware Compatibility Guide.
- ESXi7.0 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi7.0 requires a minimum of 8 GB of physical RAM. Provide at least 8 GB of RAM to run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs.
- One or more Gigabit or faster Ethernet controllers. For a list of supported network adapter models, see the VMware Compatibility Guide.
- ESXi7.0 requires a boot disk of at least 32 GB of persistent storage such as HDD, SSD, or NVMe. Use USB, SD and non-USB flash media devices only for ESXi boot bank partitions. A boot device must not be shared between ESXi hosts.
- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks are considered remote, not local. These disks are not used as a scratch partition by default because they are seen as remote.

  Note: You cannot connect a SATA CD-ROM device to a virtual machine on an ESXi host. To use the SATA CD-ROM device, you must use IDE emulation mode.

Storage Systems

For a list of supported storage systems, see the VMware Compatibility Guide. For Software Fibre Channel over Ethernet (FCoE), see Installing and Booting ESXi with Software FCoE.

ESXi Booting Requirements

vSphere 7.0 supports booting ESXi hosts from the Unified Extensible Firmware Interface (UEFI). With UEFI, you can boot systems from hard drives, CD-ROM drives, or USB media.

vSphere Auto Deploy supports network booting and provisioning of ESXi hosts with UEFI.

ESXi can boot from a disk larger than 2 TB if the system firmware and the firmware on any add-in card that you are using support it. See the vendor documentation.

Storage Requirements for ESXi7.0 Installation or Upgrade

For best performance of an ESXi7.0 installation, use a persistent storage device that is a minimum of 32 GB for boot devices. Upgrading to ESXi7.0 requires a boot device that is a minimum of 8 GB. When booting from a local disk, SAN or iSCSI LUN, at least a 32 GB disk is required to allow for the creation of system storage volumes, which include a boot partition, boot banks, and a VMFS-L based ESX-OSData volume. The ESX-OSData volume takes on the role of the legacy `/scratch` partition, locker partition for VMware Tools, and core dump destination.

Other options for best performance of an ESXi7.0 installation are the following:

- A local disk of 128 GB or larger for optimal support of ESX-OSData. The disk contains the boot partition, ESX-OSData volume and a VMFS datastore.
- A device that supports the minimum of 128 terabytes written (TBW).
- A device that delivers at least 100 MB/s of sequential write speed.
- To provide resiliency in case of device failure, a RAID 1 mirrored device is recommended.

Legacy SD and USB devices are supported with the following limitations:

- SD and USB devices are supported for boot bank partitions. For best performance, also provide a separate persistent local device with a minimum of 32 GB to store the `/scratch` and VMware Tools partitions of the ESX-OSData volume. The optimal capacity for persistent local devices is 128 GB. The use of SD and USB devices for storing ESX-OSData partitions is being deprecated.
- Starting with ESXi 7.0 Update 3, if the boot device is a USB or SD card with no local persistent storage, such as HDD, SSD, or a NVMe device, the VMware Tools partition is automatically created on the RAM disk. For more information, see Connection to the /bootbank partition intermittently breaks when you use USB or SD devices.
- If you assign the `/scratch` partition to a USB or SD card with no local persistent storage, you see warnings to prevent you from creating or configuring partitions other than the boot bank partitions on flash media devices. For best performance, set the `/scratch` partition on the RAM disk. You can also configure and move the `/scratch` partition to a SAN or NFS. For more information, see Creating a persistent scratch location for ESXi 8.x/7.x/6.x.
- You must use an SD flash device that is approved by the server vendor for the particular server model on which you want to install ESXi on an SD flash storage device. You can find a list of validated devices on partnerweb.vmware.com.
- See SD card/USB boot device revised guidance on updated guidance for SD card or USB-based environments.
- To chose a proper SD or USB boot device, see Boot device guidance for low endurance media (vSphere and vSAN).

CAUTION:

If a local disk cannot be found, or the boot media is a USB or SD device without an additional durable storage for persistent data, then the `/scratch` partition is on the RAM disk, linked to `/tmp`, and ESXi7.0 operates in degraded mode.

When in degraded mode, you see a System Alert such as: `ALERT: No persistent storage available for system logs and data. ESX is operating with limited system storage space, logs and system data will be lost on reboot.`

When ESXi7.0 operates in degraded mode, the consumption of RAM for logs might result in nonpersistent logs, possible failure to log or out of memory condition for temporary data. A possible side effect is slow booting due to the time spent for rebuilding of the disk state.

Use persistent storage of sufficient size to prevent degraded mode. You can reconfigure `/scratch` to use a separate disk or LUN.

The upgrade process to ESXi7.0 repartitions the boot device and consolidates the original core dump, locker, and scratch partitions into the ESX-OSData volume.

The following events occur during the repartitioning process:

- If a custom core dump destination is not configured, then the default core dump location is a file in the ESX-OSData volume.
- If the syslog service is configured to store log files on the 4 GB VFAT scratch partition, the log files in `var/run/log` are migrated to the ESX-OSData volume.
- VMware Tools are migrated from the locker partition and the partition is wiped.
- The core dump partition is wiped. The application core dump files that are stored on the scratch partition are deleted.

Note: Rollback to an earlier version of ESXi is not possible due to the repartitioning process of the boot device. To use an earlier version of ESXi after upgrading to version 7.0, you must create a backup of the boot device before the upgrade, and restore the ESXi boot device from the backup.

If you use USB or SD devices to perform an upgrade, the installer attempts to allocate an ESX-OSData region on an available local disk. A datastore is used for `/scratch`, if no space is available. If no local disk or datastore is found, `/scratch` is placed on the RAM disk. After the upgrade, reconfigure `/scratch` to use a persistent datastore or add a new disk for system storage volumes.

After upgrading to ESXi7.0, you can add a new local disk and enable the setting `autoPartition=TRUE` . After a reboot, the boot disk is partitioned. For more information on the boot options to configure the size of ESXi system partitions, see Boot option to configure the size of ESXi system partitions.

In Auto Deploy installations, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found, the `/scratch` partition is placed on the RAM disk. Reconfigure `/scratch` to use a persistent datastore after the installation.

For environments that boot from a SAN or use Auto Deploy, the ESX-OSData volume for each ESXi host must be set up on a separate SAN LUN. However, if `/scratch` is configured not to use ESX-OSData, you do not need to allocate a separate LUN for `/scratch` for each host. You can co-locate the scratch regions for multiple ESXi hosts onto a single LUN. The number of hosts assigned to any single LUN should be weighed against the LUN size and the I/O behavior of the virtual machines.

Supported Remote Management Server Models and Firmware Versions

You can use remote management applications to install or upgrade ESXi, or to manage hosts remotely.

Table 4: Supported Remote Management Server Models and Minimum Firmware Versions

Remote Management Server Model	Firmware Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
HP ILO 3	1.28	1.7.0_60-b19
HP ILO 4	1.13	1.7.0_60-b19
HP ILO 5	2.15	N/A
IBM RSA 2	1.03, 1.2	1.6.0_22

Recommendations for Enhanced ESXi Performance

To enhance performance, install or upgrade ESXi on a robust system with more RAM than the minimum required and with multiple physical disks.

For ESXi system requirements, see ESXi Hardware Requirements.

Table 5: Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. Provide at least 8 GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host.

System Element	Recommendation
	Operating four virtual machines with Red Hat Enterprise Linux or Windows XP requires at least 3 GB of RAM for baseline performance. This figure includes 1024 MB for the virtual machines, 256 MB minimum for each operating system as recommended by vendors. Running these four virtual machines with 512 MB RAM requires that the ESXi host have 4 GB RAM, which includes 2048 MB for the virtual machines. These calculations do not include possible memory savings from using variable overhead memory for each virtual machine. See *vSphere Resource Management*.
Dedicated Fast Ethernet adapters for virtual machines	Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.
Disk location	Place all data that your virtual machines use on physical disks allocated specifically to virtual machines. Performance is better when you do not place your virtual machines on the disk containing the ESXi boot image. Use physical disks that are large enough to hold disk images that all the virtual machines use.
VMFS6 partitioning	The ESXi installer creates the initial VMFS volumes on the first blank local disk found. To add disks or modify the original configuration, use the vSphere Client. This practice ensures that the starting sectors of partitions are 64K-aligned, which improves storage performance. **Note:** For SAS-only environments, the installer might not format the disks. For some SAS disks, it is not possible to identify whether the disks are local or remote. After the installation, you can use the vSphere Client to set up VMFS.
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 7.0 drivers. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Incoming and Outgoing Firewall Ports for ESXi Hosts

Open and close firewall ports for each service by using either the vSphere Client or the VMware Host Client.

ESXi includes a firewall that is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the host's security profile. For the list of supported ports and protocols in the ESXi firewall, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/.

The VMware Ports and Protocols Tool lists port information for services that are installed by default. If you install other VIBs on your host, additional services and firewall ports might become available. The information is primarily for services that are visible in the vSphere Client but the VMware Ports and Protocols Tool includes some other ports as well.

Required Free Space for System Logging

If you used Auto Deploy to install your ESXi7.0 host, or if you set up a log directory separate from the default location in a scratch directory on the VMFS volume, you might need to change your current log size and rotation settings to ensure that enough space is available for system logging .

All vSphere components use this infrastructure. The default values for log capacity in this infrastructure vary, depending on the amount of storage available and on how you have configured system logging. Hosts that are deployed with Auto Deploy store logs on a RAM disk, which means that the amount of space available for logs is small.

If your host is deployed with Auto Deploy, reconfigure your log storage in one of the following ways:

- Redirect logs over the network to a remote collector.
- Redirect logs to a NAS or NFS store.

If you redirect logs to non-default storage, such as a NAS or NFS store, you might also want to reconfigure log sizing and rotations for hosts that are installed to disk.

You do not need to reconfigure log storage for ESXi hosts that use the default configuration, which stores logs in a scratch directory on the VMFS volume. For these hosts, ESXi7.0 configures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 6: Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

VMware Host Client System Requirements

Make sure that your browser supports the VMware Host Client.

The following guest operating systems and Web browser versions are supported for the VMware Host Client.

Supported Browsers	Mac OS	Windows 32-bit and 64-bit	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	N/A
Safari	9.0+	N/A	N/A

ESXi Passwords and Account Lockout

For ESXi hosts, you must use a password with predefined requirements. You can change the required length and character class requirement or allow pass phrases using the Security.PasswordQualityControl advanced option. You can also set the number of passwords to remember for each user using the Security.PasswordHistory advanced option.

Note: The default requirements for ESXi passwords can change from one release to the next. You can check and change the default password restrictions by using the Security.PasswordQualityControl advanced option.

ESXi Passwords

ESXi enforces password requirements for access from the Direct Console User Interface, the ESXi Shell, SSH, or the VMware Host Client.

- By default, you must include a mix of at least three from the following four character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash when you create a password.
- By default, password length is at least 7 characters and less than 40.
- Passwords must not contain a dictionary word or part of a dictionary word.
- Passwords must not contain the user name or parts of the user name.

Note: An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used. A dictionary word used inside a password reduces the overall password strength.

Example ESXi Passwords

The following password candidates illustrate potential passwords if the option is set as follows.

```
retry=3 min=disabled,disabled,disabled,7,7
```

With this setting, a user is prompted up to three times (retry=3) for a new password that is not sufficiently strong or if the password was not entered correctly twice. Passwords with one or two character classes and pass phrases are not allowed, because the first three items are disabled. Passwords from three- and four-character classes require seven characters. See the `pam_passwdqc` man page for details on other options, such as max, passphrase, and so on.

With these settings, the following passwords are allowed.

- xQaTEhb!: Contains eight characters from three character classes.
- xQaT3#A: Contains seven characters from four character classes.

The following password candidates do not meet requirements.

- Xqat3hi: Begins with an uppercase character, reducing the effective number of character classes to two. The minimum number of required character classes is three.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. The minimum number of required character classes is three.

ESXi Pass Phrase

Instead of a password, you can also use a pass phrase. However, pass phrases are disabled by default. You can change the default setting and other settings by using the Security.PasswordQualityControl advanced option from the vSphere Client.

For example, you can change the option to the following.

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows pass phrases of at least 16 characters and at least three words.

For legacy hosts, changing the `/etc/pam.d/passwd` file is still supported, but changing the file is deprecated for future releases. Use the Security.PasswordQualityControl advanced option instead.

Changing Default Password Restrictions

You can change the default restriction on passwords or pass phrases by using the Security.PasswordQualityControl advanced option for your ESXi host. See *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

You can change the default, for example, to require a minimum of 15 characters and a minimum number of four words (passphrase=4), as follows:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

See the man page for `pam_passwdqc` for details.

Note: Not all possible combinations of password options have been tested. Perform testing after you change the default password settings.

This example sets the password complexity requirement to require eight characters from four character classes that enforce a significant password difference, a remembered history of five passwords, and a 90 day rotation policy:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Set the Security.PasswordHistory option to 5 and the Security.PasswordMaxDays option to 90.

ESXi Account Lockout Behavior

Account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of five failed attempts is allowed before the account is locked. The account is unlocked after 15 minutes by default.

Configuring Login Behavior

You can configure the login behavior for your ESXi host with the following advanced options:

- Security.AccountLockFailures. Maximum number of failed login attempts before a user's account is locked. Zero deactivates account locking.
- Security.AccountUnlockTime. Number of seconds that a user is locked out.
- Security.PasswordHistory. Number of passwords to remember for each user. Zero deactivates password history.

See the *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

Preparing for Installing ESXi

Before you install ESXi, determine the installation option that is suitable for your environment and prepare for the installation process.

- Download the ESXi Installer
- Options for Installing ESXi
- Media Options for Booting the ESXi Installer
- Using Remote Management Applications
- Customizing Installations with vSphere ESXi Image Builder
- Required Information for ESXi Installation

Download the ESXi Installer

You can obtain the ESXi installer software either from an OEM or from the Broadcom Support Portal.

Register on the Broadcom Support Portal. For more information, see Register for an account on the Broadcom Support Portal and Communities.

For product download instructions, see Download Broadcom products and software.

For download of offline bundle ZIP files for ESXi patches and updates, see Downloading Broadcom PTF files and solutions.

For more information, see VMware to Broadcom Support Frequently Asked Questions.

Options for Installing ESXi

ESXi can be installed in several ways. To ensure the best vSphere deployment, understand the options thoroughly before beginning the installation.

ESXi installations are designed to accommodate a range of deployment sizes.

Depending on the installation method you choose, different options are available for accessing the installation media and booting the installer.

Interactive ESXi Installation

Interactive installations are recommended for small deployments of fewer than five hosts.

You boot the installer from a CD or DVD, from a bootable USB device, or by PXE booting the installer from a location on the network. You follow the prompts in the installation wizard to install ESXi to disk. See Installing ESXi Interactively.

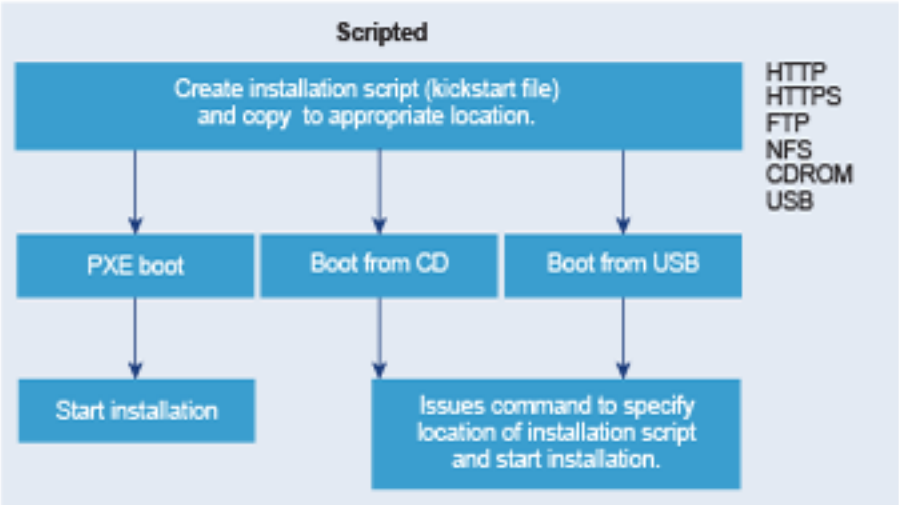
Scripted ESXi Installation

Running a script is an efficient way to deploy multiple ESXi hosts with an unattended installation.

The installation script contains the host configuration settings. You can use the script to configure multiple hosts with the same settings. See Installing or Upgrading Hosts by Using a Script.

The installation script must be stored in a location that the host can access by HTTP, HTTPS, FTP, NFS, CDROM, or USB. You can PXE boot the ESXi installer or boot it from a CD/DVD or USB drive.

Figure 3: Scripted Installation



vSphere Auto Deploy ESXi Installation

vSphere 5.x and later provide several ways to install ESXi with vSphere Auto Deploy.

vSphere Auto Deploy can provision hundreds of physical hosts with ESXi software. You can specify the image to deploy and the hosts to provision with the image. Optionally, you can specify host profiles to apply to the hosts, a vCenter Server location (datacenter, folder, or cluster), and script bundle for each host.

vCenter Server makes ESXi updates and patches available for download in the form of an image profile. The host configuration is provided in the form of a host profile. You can create host profiles by using the vSphere Client. You can

create custom image profiles by using vSphere ESXi Image Builder. See Customizing Installations with vSphere ESXi Image Builder and *vSphere Host Profiles*.

When you provision hosts by using vSphere Auto Deploy, vCenter Server loads the ESXi image directly into the host memory. vSphere Auto Deploy does not store the ESXi state on the host disk. The vSphere Auto Deploy server continues to provision this host every time the host boots.

You can also use vSphere Auto Deploy to install an ESXi host, and set up a host profile that causes the host to store the ESXi image and configuration on the local disk, a remote disk, or a USB drive. Subsequently, the ESXi host boots from this local image and vSphere Auto Deploy no longer provisions the host. This process is similar to performing a scripted installation. With a scripted installation, the script provisions a host and the host then boots from disk. For this case, vSphere Auto Deploy provisions a host and the host then boots from disk. For more information, see Use vSphere Auto Deploy for Stateless Caching and Stateful Installs.

Media Options for Booting the ESXi Installer

The ESXi installer must be accessible to the system on which you are installing ESXi.

The following boot media are supported for the ESXi installer:

- Boot from a CD/DVD. See Download and Burn the ESXi Installer ISO Image to a CD or DVD.
- Boot from a USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade.
- Boot from a network. See Network Booting the ESXi Installer.
- Boot from a remote location using a remote management application. See Using Remote Management Applications.

Download and Burn the ESXi Installer ISO Image to a CD or DVD

If you do not have an ESXi installation CD/DVD, you can create one.

You can also create an installer ISO image that includes a custom installation script. See Create an Installer ISO Image with a Custom Installation or Upgrade Script.

1. Follow the procedure Download the ESXi Installer.
2. Burn the ISO image to a CD or DVD.

Format a USB Flash Drive to Boot the ESXi Installation or Upgrade

You can format a USB flash drive to boot the ESXi installation or upgrade.

- Linux machine with superuser access to it
- USB flash drive that can be detected by the Linux machine
- The ESXi ISO image, `VMware-VMvisor-Installer-`*`version_number-build_number`*`.x86_64.iso`, which includes the `isolinux.cfg` file

The instructions in this procedure assume that the USB flash drive is detected as `/dev/sdb`.

Note: The `ks.cfg` file that contains the installation script cannot be located on the same USB flash drive that you are using to boot the installation or upgrade. The kickstart file does not have any dependency on BIOS or UEFI boot.

1. Boot Linux, log in, and enter superuser mode by using a `su` or `sudo root` command.
2. If your USB flash drive is not detected as `/dev/sdb`, or you are not sure how your USB flash drive is detected, determine how it is detected.
   a) Plug in your USB flash drive.
   b) At the command line, run the command for displaying the current log messages.

      ```
      tail -f /var/log/messages
      ```

      You see several messages that identify the USB flash drive in a format similar to the following message.

      ```
      Oct 25 13:25:23 ubuntu kernel: [  712.447080] sd 3:0:0:0: [sdb] Attached SCSI
       removable disk
      ```

      In this example, `sdb` identifies the USB device. If your device is identified differently, use that identification in place of *sdb*.
3. Overwrite the entire USB drive with the ISO image. This overwrites the partition table and any previous content on the USB drive.

   ```
   dd bs=10M if=VMware-VMvisor-Installer-version_number-build_number.x86_64.iso of=/dev/
   sdb
   ```
4. Eject the USB drive.

   ```
   eject /dev/sdb
   ```

You can use the USB flash drive to boot the ESXi installer.

Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script

You can use a USB flash drive to store the ESXi installation script or upgrade script that is used during scripted installation or upgrade of ESXi.

- Linux machine
- ESXi installation or upgrade script, the `ks.cfg` kickstart file
- USB flash drive

When multiple USB flash drives are present on the installation machine, the installation software searches for the installation or upgrade script on all attached USB flash drives.

The instructions in this procedure assume that the USB flash drive is detected as `/dev/sdb`.

Note: Do not store the `ks` file containing the installation or upgrade script on the same USB flash drive that you are using to boot the installation or upgrade.

1. Attach the USB flash drive to a Linux machine that has access to the installation or upgrade script.
2. Create a partition table.

   ```
   /sbin/fdisk /dev/sdb
   ```
   a) Type `d` to delete partitions until they are all deleted.
   b) Type `n` to create primary partition 1 that extends over the entire disk.
   c) Type `t` to set the type to an appropriate setting for the FAT32 file system, such as `c`.
   d) Type `p` to print the partition table.

      The result should be similar to the following text:

      ```
      Disk /dev/sdb: 2004 MB, 2004877312 bytes
      255 heads, 63 sectors/track, 243 cylinders
      ```

```
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         243     1951866   c   W95 FAT32 (LBA)
```

e) Type `w` to write the partition table and quit.

3. Format the USB flash drive with the FAT32 file system.

   ```
   /sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
   ```

4. Create a destination directory and mount the USB flash drive to it.

   ```
   mkdir -p /usbdisk
   mount /dev/sdb1 /usbdisk
   ```

5. Copy the ESXi installation script to the USB flash drive.

   ```
   cp ks.cfg /usbdisk
   ```

6. Unmount the USB flash drive.

   ```
   umount /usbdisk
   ```

The USB flash drive contains the installation or upgrade script for ESXi.

When you boot the ESXi installer, point to the location of the USB flash drive for the installation or upgrade script. See Enter Boot Options to Run an Installation or Upgrade Script and PXELINUX Configuration Files.

Create an Installer ISO Image with a Custom Installation or Upgrade Script

You can customize the standard ESXi installer ISO image with your own installation or upgrade script. This customization enables you to perform a scripted, unattended installation or upgrade when you boot the resulting installer ISO image.

- Linux machine
- The ESXi ISO image `VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso`,where *x.x.x* is the version of ESXi you are installing, and *XXXXXX* is the build number of the installer ISO image
- Your custom installation or upgrade script, the `KS_CUST.CFG` kickstart file

See also About Installation and Upgrade Scripts and About the boot.cfg File .

1. Download the ESXi ISO image from the Broadcom Support Portal.
2. Mount the ISO image in a folder:

   ```
   mount -o loop VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount
   ```

   `XXXXXX` is the ESXi build number for the version that you are installing or upgrading to.

3. Copy the contents of `esxi_cdrom` to another folder:

   ```
   cp -r /esxi_cdrom_mount/* /esxi_cdrom
   ```

4. Copy the kickstart file to `/esxi_cdrom`.

   ```
   cp KS_CUST.CFG /esxi_cdrom
   ```

5. Modify the `boot.cfg` file in both `/esxi_cdrom/efi/boot/boot.cfg` (for UEFI boot) and `/esxi_cdrom/boot.cfg` (for legacy BIOS boot) to specify the location of the installation or upgrade script by using the `kernelopt` option.

   You must use uppercase characters to provide the path of the script, for example,

   ```
   kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
   ```

   The installation or upgrade becomes completely automatic, without the need to specify the kickstart file during the installation or upgrade.

6. Recreate the ISO image using the `mkisofs` or the `genisoimage` command.

Command	Syntax
mkisofs	`mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -eltorito-platform efi -b EFIBOOT.IMG -no-emul-boot /esxi_cdrom`
genisoimage	`genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e EFIBOOT.IMG -no-emul-boot /esxi_cdrom`

   You can use this ISO installer image for regular boot or UEFI secure boot. However, the vSphere Lifecycle Manager cannot verify the checksum of such an ISO image and you cannot use it for upgrades by using vSphere Lifecycle Manager workflows.

The ISO image includes your custom installation or upgrade script.

Install ESXi from the ISO image.

Network Booting the ESXi Installer

You can use preboot execution environment (PXE) to boot an ESXi host from a network device, if your host uses legacy BIOS or UEFI.

Alternatively, if your ESXi host supports native UEFI HTTP, you can use hypertext transfer protocol (HTTP) to boot the host from a network device. ESXi is distributed in an ISO format that is used to install to flash memory or to a local hard drive. You can extract the files and boot them over a network interface.

PXE uses Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP) to boot an operating system over a network.

PXE booting requires some network infrastructure and a machine with a PXE-capable network adapter. Most machines that can run ESXi have network adapters that can PXE boot.

Native UEFI HTTP uses DHCP and HTTP to boot over a network. UEFI HTTP boot requires a network infrastructure, UEFI firmware version on the ESXi host that includes HTTP boot feature, and a network adapter that supports UEFI networking.

Booting by using HTTP is faster and more reliable than using TFTP. This is due to the capabilities of the TCP protocol that underlies the HTTP, such as built-in streaming and lost packet recovery. If your ESXi hosts do not support native UEFI HTTP, you can use iPXE HTTP for the boot process.

Note: Network booting with legacy BIOS firmware is possible only over IPv4. Network booting with UEFI BIOS firmware is possible over IPv4 or IPv6.

Installing and Booting ESXi with Software FCoE

You can install and boot ESXi from an FCoE LUN using VMware software FCoE adapters and network adapters with FCoE offload capabilities. Your host does not require a dedicated FCoE HBA.

Note: Starting from vSphere 7.0, VMware deprecates software FCoE adapters in production environments.

The boot LUN must not be shared between hosts and must have a size of minimum of 32 GB. See the *vSphere Storage* documentation for information about installing and booting ESXi with software FCoE.

Using Remote Management Applications

Remote management applications allow you to install ESXi on servers that are in remote locations.

Remote management applications supported for installation include HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II). For a list of currently supported server models and remote management firmware versions, see Supported Remote Management Server Models and Firmware Versions. For support on remote management applications, contact the vendor.

You can use remote management applications to do both interactive and scripted installations of ESXi remotely.

If you use remote management applications to install ESXi, the virtual CD might encounter corruption problems with systems or networks operating at peak capacity. If a remote installation from an ISO image fails, complete the installation from the physical CD media.

Customizing Installations with vSphere ESXi Image Builder

You can use VMware vSphere®ESXi™ Image Builder CLI to create ESXi installation images with a customized set of updates, patches, and drivers.

You can use vSphere ESXi Image Builder with the vSphere Client or with PowerCLI to create an ESXi installation image with a customized set of ESXi updates and patches. You can also include third-party network or storage drivers that are released between vSphere releases.

You can deploy an ESXi image created with vSphere ESXi Image Builder in either of the following ways:

- By burning it to an installation DVD.
- Through vCenter Server, using the Auto Deploy feature.

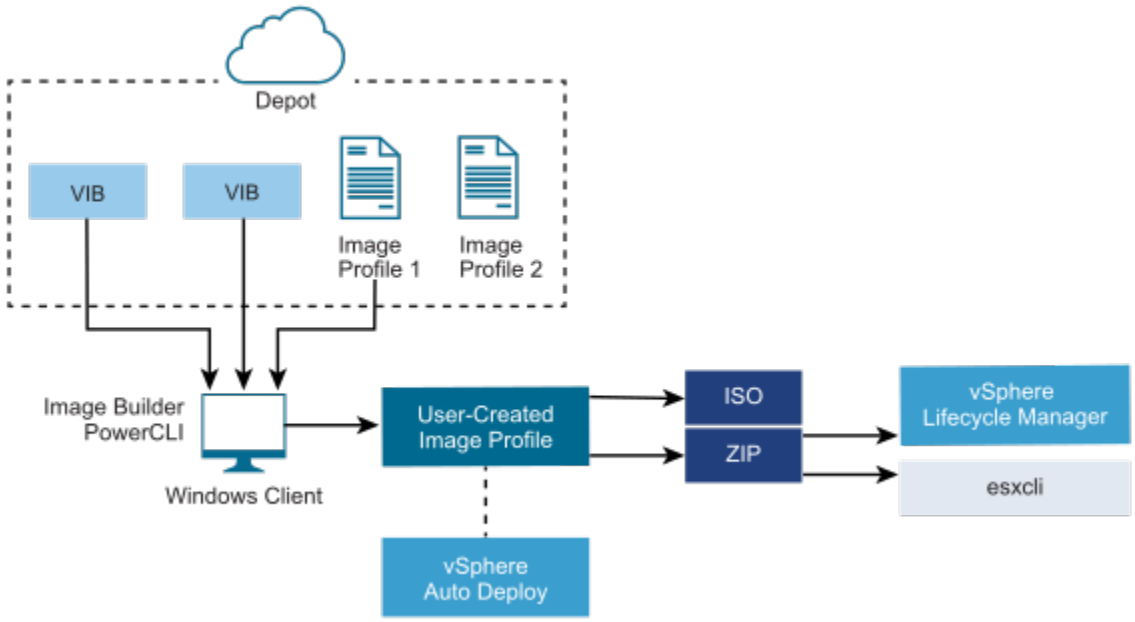
Understanding vSphere ESXi Image Builder

You can use the VMware vSphere®ESXi™ Image Builder CLI to manage software depots, image profiles, and software packages (VIBs). Image profiles and VIBs specify the software you want to use during installation or upgrade of an ESXi host.

vSphere ESXi Image Builder Overview
With vSphere ESXi Image Builder you can create ESXi image profiles for use by vSphere Auto Deploy, add custom third-party drivers to existing image profiles and export to ISO or bundle, and perform upgrades.

For basic concepts related to the way VMware vSphere software is created, packaged, and distributed, see Bulletins, Components, Add-Ons, and ESXi Base Images.

Figure 4: Image Builder Architecture



You use vSphere ESXi Image Builder cmdlets for managing the software to deploy to your ESXi hosts in several different situations.

Table 7: Cases Where You Can Use vSphere ESXi Image Builder

Use Case for vSphere ESXi Image Builder	Description
Create image profiles for use by vSphere Auto Deploy	Use vSphere ESXi Image Builder to create an image profile that defines the VIBs that vSphere Auto Deploy uses to provision hosts.
Add custom third-party drivers to existing image profile and export to ISO or bundle	When you add a third-party driver or extension custom VIBs to your ESXi hosts, use vSphere ESXi Image Builder to clone the base image provided by VMware, add the custom VIBs, and export to ISO or to offline bundle ZIP file.
Perform upgrades	If you upgrade a system that includes custom extensions or drivers, you can use vSphere ESXi Image Builder to create a custom image profile that includes vSphere 6.7 compatible VIBs for the custom extensions. Export the custom image profile to an ISO or to a ZIP to upgrade your system by using Update Manager baselines.
Create custom images with reduced footprint	If you require a minimal footprint image, you can clone the ESXi base image profile and remove VIBs using vSphere ESXi Image Builder.

The vSphere ESXi Image Builder cmdlets take image profiles and VIBs as input and produce various outputs.

Table 8: Input and Output to the vSphere ESXi Image Builder Cmdlets

Parameter	Description
Input	Image profiles and VIBs that are located in a software depot are used as input to PowerCLI cmdlets running on a Windows client.
Output	PowerCLI cmdlets create custom image profiles that can be exported to an ISO image or an offline depot ZIP file. ISO images are used for installation. The ZIP depot can be used by Update Manager or by `esxcli software` commands to update or install images. Image profiles are also used in vSphere Auto Deploy rules to customize the software to provision ESXi hosts with.

Watch the video "Using Image Builder CLI" for information about vSphere ESXi Image Builder:

VMware.ImageBuilder Cmdlets Overview

The VMware.Image Builder component of VMware PowerCLI provides cmdlets for managing VIBs, image profiles, and other content in software depots.

vSphere 7.0 introduced new ways of packaging VIBs along with legacy bulletins and patches, and software depots contain base images, vendor addons and components, along with VIBs and image profiles. VMware PowerCLI 12.0 and later provide cmdlets that work with the new content in software depots.

VMware.ImageBuilder includes the following cmdlets.

Note: When you run VMware.ImageBuilder cmdlets, provide all parameters on the command line when you invoke the cmdlet. Supplying parameters in interactive mode is not recommended.

Run `Get-Help` *`cmdlet_name`* at the PowerCLI prompt for detailed reference information.

Table 9: VMware.ImageBuilder Cmdlets Used with Legacy Content in Software Depots

Cmdlet	Description
`Add-EsxSoftwareDepot`	Adds the software depot or ZIP file at the specified location to your current environment. Downloads metadata from the depot and analyzes VIBs for dependencies.
`Remove-EsxSoftwareDepot`	Disconnects from the specified software depot.
`Get-EsxSoftwareDepot`	Returns a list of software depots that are in the current environment. If you want to examine and manage image profiles and VIBs, you must first add the corresponding software depot to your environment.
`Get-EsxSoftwarePackage`	Returns a list of software package objects (VIBs). Use this cmdlet's options to filter the results.
`Get-EsxImageProfile`	Returns an array of `ImageProfile` objects from all currently added depots.
`New-EsxImageProfile`	Creates a new image profile. In most cases, creating a new profile by cloning an existing profile is recommended. See Clone an Image Profile with PowerCLI Cmdlets.
`Set-EsxImageProfile`	Modifies a local `ImageProfile` object and performs validation tests on the modified profile. The cmdlet returns the modified object but does not persist it.
`Export-EsxImageProfile`	Exports an image profile as either an ESXi ISO image for ESXi installation, or as a ZIP file.
`Compare-EsxImageProfile`	Returns an `ImageProfileDiff` structure that shows whether the two profiles have the same VIB list and acceptance level. See Acceptance Levels.
`Remove-EsxImageProfile`	Removes the image profile from the software depot.

Cmdlet	Description
`Add-EsxSoftwarePackage`	Adds one or more new packages (VIBs) to an existing image profile.
`Remove-EsxSoftwarePackage`	Removes one or more packages (VIBs) from an image profile.
`Set-ESXImageProfileAssociation`	Associates the specified image profile with the specified ESXi system.

Table 10: VMware.ImageBuilder Cmdlets Used with New Content in Software Depots

Cmdlet	Description
`Get-DepotAddons`	Retrieves an array of objects that provide basic information about addons in a software depot.
`Get-DepotBaseImages`	Retrieves an array of objects that provide basic information about base images in a software depot.
`Get-DepotComponents`	Retrieves an array of objects that provide basic information about components in a software depot.
`Get-DepotInfo`	Retrieves basic information about the software depot located at the specified file path or URL address.
`Get-DepotVibs`	Retrieves an array of objects that provide basic information about VIBs in a software depot.
`New-IsoImage`	Generates an ISO image by using the specified software depot and software specification at the specified file path.
`New-PxeImage`	Generates a PXE image by using the specified software depot and software specification at the specified file path.

Image Profiles

Image profiles define the set of VIBs that an ESXi installation or update process uses. Image profiles apply to ESXi hosts provisioned with vSphere Auto Deploy. You define and manipulate image profiles with vSphere ESXi Image Builder.

Image Profile Requirements

You can create a custom image profile from scratch or clone an existing profile and add or remove VIBs. A profile must meet the following requirements to be valid.

- Each image profile must have a unique name and vendor combination.
- Each image profile has an acceptance level. When you add a VIB to an image profile with an vSphere ESXi Image Builder cmdlet, Image Builder checks that the VIB matches the acceptance level defined for the profile.
- You cannot remove VIBs that are required by other VIBs.
- You cannot include two versions of the same VIB in an image profile. When you add a new version of a VIB, the new version replaces the existing version of the VIB.

Image Profile Validation

An image profile and its VIBs must meet several criteria to be valid.

- Image profiles must contain at least one base VIB and one bootable kernel module.
- If any VIB in the image profile depends on another VIB, that other VIB must also be included in the image profile. VIB creators store that information in the SoftwarePackage object's Depends property.
- VIBs must not conflict with each other. VIB creators store conflict information in the SoftwarePackage object's Conflicts property.
- Two VIBs with the same name, but two different versions, cannot coexist. When you add a new version of a VIB, the new version replaces the existing version of the VIB.

- No acceptance level validation issues exist.

When you make a change to an image profile, vSphere ESXi Image Builder checks that the change does not invalidate the profile.

Dependency Validation	When you add or remove a VIB, vSphere ESXi Image Builder checks that package dependencies are met. Each SoftwarePackage object includes a Depends property that specifies a list of other VIBs that VIB depends on. See Structure of ImageProfile, SoftwarePackage, and ImageProfileDiff Objects
Acceptance Level Validation	vSphere ESXi Image Builder performs acceptance level validation each time an image profile is created or changed. vSphere ESXi Image Builder checks the acceptance level of VIBs in the image profile against the minimum allowed acceptance level of the profile. The acceptance level of the VIB is also validated each time the signature of a VIB is validated.

VIB Validation During Export

When you export an image profile to an ISO, vSphere ESXi Image Builder validates each VIB by performing the following actions.

- Checks that no conflicts exist by checking the Conflicts property of each SoftwarePackage object.
- Performs VIB signature validation. Signature validation prevents unauthorized modification of VIB packages. The signature is a cryptographic checksum that guarantees that a VIB was produced by its author. Signature validation also happens during installation of VIBs on an ESXi host and when the vSphere Auto Deploy server uses VIBs.
- Checks that VIBs follow file path usage rules. VMware tests VMwareCertified and VMwareAccepted VIBs to guarantee those VIBs always follow file path usage rules.

Acceptance Levels

Each VIB is released with an acceptance level that cannot be changed. The host acceptance level determines which VIBs can be installed to a host. You can change the host acceptance levels with `esxcli` commands.

VMware supports the following acceptance levels.

VMwareCertified	The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only I/O Vendor Program (IOVP) program drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.
VMwareAccepted	VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plug-ins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
PartnerSupported	VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
CommunitySupported	The CommunitySupported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs.

VIBs at this level have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

Structure of ImageProfile, SoftwarePackage, and ImageProfileDiff Objects

Knowing the structure of `ImageProfile`, `SoftwarePackage`, and `ImageProfileDiff` objects helps you manage deployment and upgrade processes.

ImageProfile Object Properties

The `ImageProfile` object, which is accessible with the `Get-EsxImageProfile`PowerCLI cmdlet, has the following properties.

Name	Type	Description
`AcceptanceLevel`	`AcceptanceLevel`	Determines which VIBs you can add to the profile. Levels are VMwareCertified, VMwareAccepted, PartnerSupported, and CommunitySupported. See Working with Acceptance Levels.
`Author`	`System.String`	The person who created the profile. 60 characters or fewer.
`CreationTime`	`System.DateTime`	The timestamp of creation time.
`Description`	`System.String`	The full text description of profile. No length limit.
`GUID`	`System.String`	Globally unique ID of the image profile.
`ModifiedTime`	`System.DateTime`	The timestamp of last modification time.
`Name`	`System.String`	The name of the image profile. 80 characters or fewer.
`ReadOnly`	`System.Boolean`	When set to `true` , the profile cannot be edited. Use `Set-EsxImageProfile -Readonly` to make your custom image profiles read-only.
`Rules`	`ImageProfileRule[]`	Any OEM hardware requirements and restrictions that the image profile might have. vSphere Auto Deploy verifies the value of this property when deploying an image profile and deploys the profile if matching hardware is available.
`Vendor`	`System.String`	The organization that publishes the profile. 40 characters or fewer.
`VibList`	`SoftwarePackage[]`	The list of VIB IDs the image contains.

SoftwarePackage Object Properties

When preparing an image profile, you can examine software packages to decide which packages are suitable for inclusion. The `SoftwarePackage` object has the following properties.

Name	Type	Description
`AcceptanceLevel`	`AcceptanceLevel`	The acceptance level of this VIB.
`Conflicts`	`SoftwareConstraint[]`	A list of VIBs that cannot be installed at the same time as this VIB. Each constraint uses the following format: `package-name[<<|<=|=|>=|<< version]`

Name	Type	Description
Depends	SoftwareConstraint[]	A list of VIBs that must be installed at the same time as this VIB. Same constraint format as Conflicts property.
Description	System.String	The long description of the VIB.
Guid	System.String	The unique ID for the VIB.
LiveInstallOk	System.Boolean	True if live installs of this VIB are supported.
LiveRemoveOk	System.Boolean	True if live removals of this VIB are supported.
MaintenanceMode	System.Boolean	True if hosts must be in maintenance mode for installation of this VIB.
Name	System.String	The name of the VIB. Usually uniquely describes the package on a running ESXi system.
Provides	SoftwareProvides	The list of virtual packages or interfaces this VIB provides. See SoftwareProvide Object Properties.
ReferenceURLs	SupportReference[]	The list of SupportReference objects with in-depth support information. The SupportReference object has two properties, Title and URL, both of type System.String.
Replaces	SoftwareConstraint[]	The list of SoftwareConstraint objects that identify VIBs that replace this VIB or make it obsolete. VIBs automatically replace VIBs with the same name but lower versions.
ReleaseDate	System.DateTime	Date and time of VIB publication or release.
SourceUrls	System.String[]	The list of source URLs from which this VIB can be downloaded.
StatelessReady	System.Boolean	True if the package supports host profiles or other technologies that make it suitable for use in conjunction with vSphere Auto Deploy.
Summary	System.String	A one-line summary of the VIB.
Tags	System.String[]	An array of string tags for this package defined by the vendor or publisher. Tags can be used to identify characteristics of a package.
Vendor	System.String	The VIB vendor or publisher.
Version	System.String	The VIB version.
VersionObject	Software.Version	The VersionObject property is of type SoftwareVersion. The SoftwareVersion class implements a static Compare method to compare two versions of strings. See SoftwareVersion Object Properties

ImageProfileDiff Object Properties

When you run the Compare-EsxImageProfile cmdlet, you pass in two parameters, first the reference profile, and then the comparison profile. The cmdlet returns an ImageProfileDiff object, which has the following properties.

Name	Type	Description
CompAcceptanceLevel	System.String	The acceptance level for the second profile that you passed to Compare-EsxImageProfile.
DowngradeFromRef	System.String[]	The list of VIBs in the second profile that are downgrades from VIBs in the first profile.
Equal	System.Boolean	True if the two image profiles have identical packages and acceptance levels.
OnlyInComp	System.String	The list of VIBs found only in the second profile that you passed to Compare-EsxImageProfile.
OnlyInRef	System.String[]	The list of VIBs found only in the first profile that you passed to Compare-EsxImageProfile.
PackagesEqual	System.Boolean	True if the image profiles have identical sets of VIB packages.
RefAcceptanceLevel	System.String	The acceptance level for the first profile that you passed to Compare-EsxImageProfile.
UpgradeFromRef	System.String[]	The list of VIBs in the second profile that are upgrades from VIBs in the first profile.

SoftwareVersion Object Properties

The SoftwareVersion object lets you compare two version strings. The object includes a Comparestatic method that accepts two strings as input and returns 1 if the first version string is a higher number than the second version string. Compare returns 0 if two versions strings are equal. Compare returns -1 if the second version string is a higher number than the first string. The object has the following properties.

Name	Type	Description
Version	System.String	The part of the version before the hyphen. This part indicates the primary version.
Release	System.String	The part of the version after the hyphen. This part indicates the release version.

SoftwareConstraint Object Properties

The SoftwareConstraint object implements a MatchesProvide method. The method accepts a SoftwareProvides or SoftwarePackage object as input and returns True if the constraint matches the SoftwareProvide or the SoftwarePackage, or returns False otherwise.

The SoftwareConstraint object includes the following properties.

Name	Type	Description
Name	System.String	The name of the constraint. This name should match a corresponding SoftwareProvideName property.
Relation	System.String	An enum, or one of the following comparison indicators: <<, <=, = >=, >>. This property can be $null if the constraint does not have a Relation and Version property.
Version	System.String	The version to match the constraint against. This property can be $null if the

Name	Type	Description
		constraint does not have a `Relation` and `Version` property.
`VersionObject`	`SoftwareVersion`	The version represented by a `SoftwareVersion` object.

SoftwareProvide Object Properties

The `SoftwareProvide` object includes the following properties.

Name	Type	Description
`Name`	`System.String`	The name of the provide.
`Version`	`System.String`	The version of the provide. Can be $null if the provide does not specify a version.
`Release`	`System.String`	The version of the provide as represented by a SoftwareVersion object. See SoftwareVersion Object Properties.

vSphere ESXi Image Builder Installation and Usage

vSphere ESXi Image Builder consists of the vSphere ESXi Image Builder server and the vSphere ESXi Image Builder PowerShell cmdlets. The vSphere ESXi Image Builder server starts when your run the first vSphere ESXi Image Builder cmdlet.

Install vSphere ESXi Image Builder and Prerequisite Software

Before you can run vSphere ESXi Image Builder cmdlets, you must install PowerCLI and all prerequisite software. The vSphere ESXi Image Builder snap-in is included with the PowerCLI installation.

If you want to manage vSphere ESXi Image Builder with PowerCLI cmdlets, verify that Microsoft .NET Framework 4.5 or 4.5.x and Windows PowerShell 3.0 or 4.0 are installed on a Microsoft Windows system. See the PowerCLI User's Guide.

1. Open PowerShell on your workstation.
2. Download a version of PowerCLI later than PowerCLI 6.5R1 from the PowerCLI home page.
3. To install all PowerCLI modules, run the command: `Install-Module VMware.PowerCLI -Scope CurrentUser` . Alternatively, you can install individual PowerCLI modules by running the Install-Module cmdlet with the module name.If you see a warning that you are installing modules from an untrusted repository, press **y** and then press **Enter** to confirm the installation.

   You can verify that the PowerCLI module is available by using the command

   `Get-Module -Name VMware.PowerCLI -ListAvailable .`

Review Using VMware.Image Builder Cmdlets .If you are new to PowerCLI, read the *PowerCLIUser's Guide*.

Use vSphere ESXi Image Builder cmdlets and other PowerCLI cmdlets and PowerShell cmdlets to manage image profiles and VIBs. Use `Get-Help` *`cmdlet_name`* at any time for command-line help.

Configure the vSphere ESXi Image Builder

Before you can use vSphere ESXi Image Builder with the vSphere Client, you must verify that the service is enabled and running.

- Verify that you have enough storage for the vSphere Auto Deploy repository. The vSphere Auto Deploy server uses the repository to store data it needs, including the rules and rule sets you create and the VIBs and image profiles that you specify in your rules.
  Best practice is to allocate 2 GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 400 MB. Determine how much space to reserve for the vSphere Auto Deploy repository by considering how many image profiles you expect to use.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Auto Deploy** page, select your vCenter Server from the drop-down menu at the top.
3. Click **Enable Image Builder** to activate the service.
   The **Software Depot** page appears.

- Add a Software Depot.
- Import a Software Depot.
- Clone an Image Profile.
- Create an Image Profile.
- Prepare Your System for vSphere Auto Deploy.

- You can change the default configuration properties of the **Image Builder Service**. For more information, see "Configuring vCenter Server" in the *vCenter Server and Host Management* documentation.

Using VMware.Image Builder Cmdlets
With VMware.Image Builder cmdlets, you can take advantage of all PowerCLI features.

VMware.Image Builder cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. You can take advantage of all PowerCLI features by using VMware.Image Builder cmdlets. Experienced PowerShell users can use VMware.Image Builder cmdlets just like other PowerShell cmdlets. If you are new to PowerShell and PowerCLI, follow these tips.

You can type cmdlets, parameters, and parameter values in the PowerCLI shell.

- Get help for any cmdlet by running `Get-Help` *`cmdlet_name`*.
- Remember that PowerShell is not case sensitive.
- Use tab completion for cmdlet names and parameter names.
- Format any variable and cmdlet output by using `Format-List` or `Format-Table` or their short forms `fl` or `ft`. See `Get-Help Format-List`.
- Use wildcards for searching and filtering VIBs and image profiles. All wildcard expressions are supported.

Passing Parameters by Name

You can pass in parameters by name in most cases and surround parameter values that contain spaces or special characters with double quotes.

```
Add-EsxSoftwarePackage -ImageProfile profile42 -SoftwarePackage "partner package 35"
```

Passing Parameters as Objects

You can pass parameters as objects if you want to do scripting and automation. You can use the technique with cmdlets that return multiple objects or with cmdlets that return a single object.

1. Bind the output of a cmdlet that returns multiple objects to a variable.
   ```
   $profs = Get-EsxImageProfile
   ```
2. When you run the cmdlet that needs the object as input, access the object by position, with the list starting with 0.
   ```
   Add-EsxSoftwarePackage -ImageProfile $profs[4] -SoftwarePackage partner-pkg
   ```

The example adds the specified software package to the fifth image profile in the list returned by `Get-EsxImageProfile`.

Most of the examples in the *vCenter Server Installation and Setup* documentation pass in parameters by name. vSphere ESXi Image Builder Workflows with PowerCLI Cmdlets includes examples that pass parameters as objects.

Using vSphere ESXi Image Builder with the vSphere Client

You can manage software packages (VIBs), image profiles, and software depots by using the vSphere ESXi Image Builder service in the vSphere Client.

Add a Software Depot

Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Before you can work with software depots and customize image profiles, you must add one or more software depots to the vSphere ESXi Image Builder inventory. You can add a software depot by using the vSphere Client.

Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder in the vSphere Web Client.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.

2. On the **Software Depots** tab, click **New**.

   The **Add Software Depot** window appears.

   Note:

   The URLs of the official VMware online depot are now unique for each customer. To update the download sources URLs, see the following KB articles: 390121 and 390123.

3. Select the type of depot that you want to create.

Option	Action
Online Depot	1. Enter a name of the depot in the inventory. 2. Enter the URL of the online depot.
Custom Depot	Enter the name of the depot in the inventory.

   The VMware online software depot is located at https://dl.broadcom.com/<Download Token>/PROD/COMP/ESX_HOST/main/vmw-depot-index.xml

4. Click **Add**.
5. Optional: Click the **Software Packages** tab to view the contents of the selected depot and additional information about the packages.
6. Optional: If you added an **Online depot**, you can also:
   - **Check for Updates** to get the latest depot packages.
   - Click **More info** to get additional depot details.

The software depot is added to the list.

- You can associate an image profile with a new vSphere Auto Deploy rule to provision ESXi hosts. See Create a Deploy Rule or Clone a Deploy Rule.
- You can associate an image profile with an ESXi host. See Add a Host to the vSphere Auto Deploy Inventory.
- Edit the Image Profile Association of a Host
- **Remove** a custom software depot.

Related Links

Import a Software Depot on page 1007
If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008
Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009
You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015
If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Import a Software Depot

If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

If an offline depot is located on your local file system, you can import the ZIP file to the vSphere ESXi Image Builder inventory by using the vSphere Client.

Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.
2. On the **Software Depots** tab, click **Import** .
3. Enter the name of the software depot in the inventory.
4. Click **Browse** and select a ZIP file from the local system, that contains the software depot you want to import.
5. Click **Upload**.

- You can associate an image profile with a new vSphere Auto Deploy rule to provision ESXi hosts. See Create a Deploy Rule or Clone a Deploy Rule.
- You can associate an image profile with an ESXi host. See Add a Host to the vSphere Auto Deploy Inventory .
- Edit the Image Profile Association of a Host.

Related Links

Add a Software Depot on page 1006
Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Clone an Image Profile on page 1008
Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009

You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015
If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Clone an Image Profile
Use the vSphere Client to clone image profiles.

You can use the vSphere Client to clone image profiles. You can clone an image profile when you want to make small changes to the VIB list in a profile, or if you want to use hosts from different vendors and want to use the same basic profile, but want to add vendor-specific VIBs.

- Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.
- Add or import a software depot to the vSphere ESXi Image Builder inventory. See Add a Software DepotAdd a Software Depotor Import a Software Depot.
- Verify that there is at least one custom depot in the vSphere ESXi Image Builder inventory.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.
2. On the **Software Depots** tab, use the drop-down menu to select the software depot that contains the image profile that you want to work with.
3. From the list of image profiles in the depot, select the image profile that you want to clone and click **Clone**.
4. Enter an image profile name, vendor, and description.
   You must enter a unique image profile name.
5. From the **Software depot** drop-down menu, select in which custom depot to add the new image profile.
6. Click **Next**.
   The **Select software packages** page appears.
7. From the drop-down menu, select an acceptance level for the image profile.
   The acceptance level of the VIBs you add to the base image must be at least as high as the level of the base image. If you add a VIB with a lower acceptance level to the image profile, you must lower the image profile acceptance level. For more information, see Working with Acceptance Levels.

8. Select the VIBs that you want to add to the image profile and deselect the ones that you want to remove, and click **Next**.

   Note: The image profile must contain a bootable ESXi image to be valid.

   vSphere ESXi Image Builder verifies that the change does not invalidate the profile. Some VIBs depend on other VIBs and become invalid if you include them in an image profile separately. When you add or remove a VIB, vSphere ESXi Image Builder checks whether the package dependencies are met.

9. On the **Ready to complete** page, review the summary information for the new image profile and click **Finish**.

- You can associate an image profile with a new vSphere Auto Deploy rule to provision ESXi hosts. See Create a Deploy Rule or Clone a Deploy Rule.
- You can associate an image profile with an ESXi host. See Add a Host to the vSphere Auto Deploy Inventory .
- Edit the Image Profile Association of a Host.

Related Links

Add a Software Depot on page 1006
Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007
If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Create an Image Profile on page 1009
You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015
If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Create an Image Profile

You can create a new image profile by using the vSphere Client instead of cloning an existing one.

You might consider creating a new image profile if it differs significantly from the image profiles in your inventory.

- Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.
- Add or import a software depot to the vSphere ESXi Image Builder inventory. See Add a Software DepotAdd a Software Depotor Import a Software Depot.
- Verify that there is at least one custom depot in the vSphere ESXi Image Builder inventory.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.

2. From the **Software depot** drop-down menu, select in which custom depot to add the new image profile.
3. On the Image Profiles tab, click **New Image Profile**.
4. Enter an image profile name, vendor, and description.
   You must enter a unique image profile name.
5. Click **Next**.
   The **Select software packages** page appears.
6. From the drop-down menu, select an acceptance level for the image profile.
   The acceptance level of the VIBs you add to the base image must be at least as high as the level of the base image. If you add a VIB with a lower acceptance level to the image profile, you must lower the image profile acceptance level. For more information, see Working with Acceptance Levels.
7. Select the VIBs that you want to add to the image profile and deselect the ones that you want to remove, and click **Next**.

   Note: The image profile must contain a bootable ESXi image to be valid.

   vSphere ESXi Image Builder verifies that the change does not invalidate the profile. Some VIBs depend on other VIBs and become invalid if you include them in an image profile separately. When you add or remove a VIB, vSphere ESXi Image Builder checks whether the package dependencies are met.
8. On the **Ready to complete** page, review the summary information for the new image profile and click **Finish**.

- You can associate an image profile with a new vSphere Auto Deploy rule to provision ESXi hosts. See Create a Deploy Rule or Clone a Deploy Rule.
- You can associate an image profile with an ESXi host. See Add a Host to the vSphere Auto Deploy Inventory .
- Edit the Image Profile Association of a Host.
- Select and **Delete** an Image profile.
- **View Software Packages** for the selected image profile.

Related Links

Add a Software Depot on page 1006
Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007
If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008
Use the vSphere Client to clone image profiles.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015

If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Edit an Image Profile

You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

- Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.
- Add or import a software depot to the vSphere ESXi Image Builder inventory. See Add a Software DepotAdd a Software Depotor Import a Software Depot.
- Verify that there is at least one custom depot in the vSphere ESXi Image Builder inventory.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.
2. On the **Software Depots** tab, use the drop-down menu to select the software depot that contains the image profile that you want to work with.
3. On the **Image Profiles** tab, select the image profile that you want to edit and click **Edit**.

   The **Edit Image Profile** wizard appears.
4. Optional: Change the name, vendor and description information of the image profile.
5. Click **Next**.

   The **Select software packages** page appears.
6. From the drop-down menu, select an acceptance level for the image profile.

   The acceptance level of the VIBs you add to the base image must be at least as high as the level of the base image. If you add a VIB with a lower acceptance level to the image profile, you must lower the image profile acceptance level. For more information, see Working with Acceptance Levels.
7. Select the VIBs that you want to add to the image profile and deselect the ones that you want to remove, and click **Next**.

   Note: The image profile must contain a bootable ESXi image to be valid.

   vSphere ESXi Image Builder verifies that the change does not invalidate the profile. Some VIBs depend on other VIBs and become invalid if you include them in an image profile separately. When you add or remove a VIB, vSphere ESXi Image Builder checks whether the package dependencies are met.
8. On the **Ready to complete** page, review the summary information for the edited image profile and click **Finish**.

- You can associate an image profile with a new vSphere Auto Deploy rule to provision ESXi hosts. See Create a Deploy Rule or Clone a Deploy Rule.
- You can associate an image profile with an ESXi host. See Add a Host to the vSphere Auto Deploy Inventory .
- Edit the Image Profile Association of a Host.

Related Links

Add a Software Depot on page 1006

Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007

If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008

Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009

You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015
If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Compare Image Profiles

You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

- Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.
- Add or import a software depot to the vSphere ESXi Image Builder inventory. See Add a Software DepotAdd a Software Depotor Import a Software Depot.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.
2. On the **Software Depots** tab, use the drop-down menu to select the software depot that contains the image profile that you want to work with.
3. On the **Image Profiles** tab, select an image profile and click **Compare To**.

   The **Compare Image Profile** wizard appears.
4. Click **Change** to select a second image profile.

   The **Select Image Profile** page appears.
5. Select a software depot from the drop-down menu and click on the second image profile.
6. In the **Compare Image Profile** page, select a comparison option from the **Software packages** drop-down menu.

   The left side of the list displays details of the VIBs that the first chosen image profile contains. The right part of the list provides information about the second image profile. The VIBs marked as `Same` are identical in both profiles. VIBs that are present in one of the image profiles are marked as `Missing` next to the image profile that they are not present in.

Related Links

Add a Software Depot on page 1006
Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007
If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008
Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009
You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011

You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015
If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Move an Image Profile to a Different Software Depot

You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

- Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.
- Add or import a software depot to the vSphere ESXi Image Builder inventory. See Add a Software DepotAdd a Software Depotor Import a Software Depot.
- Verify that there is at least one custom depot in the vSphere ESXi Image Builder inventory.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.
2. On the **Software Depots** tab, use the drop-down menu to select the software depot that contains the image profile that you want to work with.
3. On the **Image Profiles** tab, select an image profile and click **Move to**.
4. From the drop-down menu, select the custom depot in which you want to move the image profile.
5. Click **OK**.

The image profile is in the new software depot.

Related Links

Add a Software Depot on page 1006
Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007
If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008
Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009
You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Regenerate an Image Profile on page 1015

If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Export an Image Profile to ISO or Offline Bundle ZIP

You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

You can export an image profile to an ISO image or a ZIP file by using the vSphere Client. You can use the ISO image as an ESXi installer or to upgrade hosts with vSphere Lifecycle Manager. The ZIP file contains metadata and the VIBs of the image profile. You can use it for ESXi upgrades or as an offline depot.

- Verify that the vSphere ESXi Image Builder service is enabled and running. See Configure the vSphere ESXi Image Builder.
- Add or import a software depot to the vSphere ESXi Image Builder inventory. See Add a Software DepotAdd a Software Depotor Import a Software Depot.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere ESXi Image Builder service.
2. On the **Software Depots** tab, use the drop-down menu to select the software depot that contains the image profile that you want to work with.
3. On the **Image Profiles** tab, select the image profile that you want to export and click **Export**.

   The **Export Image Profile** window appears.
4. Select the type of the exported file.

Option	Description
ISO	Exports the image profile to a bootable ISO image. If you want to create an ISO image that you can burn to a CD or DVD and use to start a stateless ESXi instance, select the **Do not include an installer on the ISO** check box.
ZIP	Exports the image profile to a ZIP file.

5. Optional: If you want to bypass the acceptance level verification of the image profile, select **Skip acceptance level checking**.
6. Click **Ok**.

   The **Download** link starts generating in the "Download Image Profiles" column of the selected image profile.
7. When the image generates successfully, click **Download** to save the exported file.

- You can associate an image profile with a new vSphere Auto Deploy rule to provision ESXi hosts. See Create a Deploy Rule or Clone a Deploy Rule.
- You can associate an image profile with an ESXi host. See Add a Host to the vSphere Auto Deploy Inventory .
- Edit the Image Profile Association of a Host.

Related Links

Add a Software Depot on page 1006

Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007

If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008

Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009

You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Regenerate an Image Profile on page 1015
If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

Regenerate an Image Profile

If you use Auto Deploy to add stateful ESXi hosts to a cluster that you manage by using an image, all hosts must have the same software specification.

When an Auto Deploy rule is created and the target cluster is managed by an image, a Preboot Execution Environment (PXE) image is created based on the image specification of the cluster. The generated PXE image is cached and is not automatically updated. As a result, if you modify the image specification in the vSphere Lifecycle Manager, you must update the PXE image manually.

For information how to create a rule to add hosts to a cluster managed by an image, see *Use Auto Deploy to Add a Host to a Cluster Managed by an Image* from the *vSphere Lifecycle Manager* documentation.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, select the desired rule.
   You must select a rule, which matches ESXi hosts to a cluster that you manage by an image.
3. If the rule is active, first you must deactivate the rule.
   a) Click the **Activate/Deactive Rules** tab
   b) In the dialog box, select the rule.
   c) In the dialog box, select **Deactivate** and click **OK**.
4. Select **Reacreate Image Profile** and in the confirmation dialog box, click **Recreate**.
5. Optional: Activate the rule again.
   a) Click the **Activate/Deactive Rules** tab
   b) In the dialog box, select the rule.
   c) In the dialog box, select **Activate** and click **OK**.

The PXE image is running the latest image specification.

Related Links

Add a Software Depot on page 1006
Add one or more software depots to the vSphere ESXi Image Builder inventory to customize image profiles.

Import a Software Depot on page 1007
If an offline depot is located on your local file system, import the ZIP file to the vSphere ESXi Image Builder inventory.

Clone an Image Profile on page 1008
Use the vSphere Client to clone image profiles.

Create an Image Profile on page 1009
You can create a new image profile by using the vSphere Client instead of cloning an existing one.

Edit an Image Profile on page 1011
You can edit image profiles by using the vSphere Client. You can change the name, details and VIB list of an image profile.

Compare Image Profiles on page 1012
You can compare two image profiles by using the vSphere Client to check if they have the same VIB list, version, or acceptance level.

Move an Image Profile to a Different Software Depot on page 1013
You can move image profiles between custom depots by using the vSphere Client and modify it without affecting the source depot's configuration.

Export an Image Profile to ISO or Offline Bundle ZIP on page 1014
You can export an image profile to an ISO image or a ZIP file by using the vSphere Client.

Using vSphere ESXi Image Builder with PowerCLI Cmdlets

The VMware.Image Builder component of VMware PowerCLI provides cmdlets that allow you to manipulate software depots, image profiles, and VIBs.

Clone an Image Profile with PowerCLI Cmdlets

Cloning a published profile is the easiest way to create a custom image profile. Cloning a profile is especially useful if you want to remove a few VIBs from a profile, or if you want to use hosts from different vendors and want to use the same basic profile, but want to add vendor-specific VIBs. VMware partners or large installations might consider creating a new profile.

- Install the PowerCLI and all prerequisite software. See vSphere ESXi Image Builder Installation and Usage.
- Verify that you have access to the software depot that contains the image profile you want to clone.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Optional: Run the `Get-EsxImageProfile` cmdlet to find the name of the profile that you want to clone.

   You can use filtering options with `Get-EsxImageProfile`.

3. Run the `New-EsxImageProfile` cmdlet to create the new profile and use the `-CloneProfile` parameter to specify the profile you want to clone.

   ```
   New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"
   ```

   This example clones the profile named *My_Profile* and assigns it the name Test Profile 42. You must specify a unique combination of name and vendor for the cloned profile.

See Examine Depot Contents for some examples of filtering.

Customize the image profile by adding or removing VIBs. See Add VIBs to an Image Profile with PowerCLI Cmdlets.

Add VIBs to an Image Profile with PowerCLI Cmdlets

You can add one or more VIBs to an image profile if that image profile is not set to read only. If the new VIB depends on other VIBs or conflicts with other VIBs in the profile, a message is displayed at the PowerShell prompt and the VIB is not added.

Install the PowerCLI and all prerequisite software. See Install vSphere ESXi Image Builder and Prerequisite Software

You can add VIBs from VMware or from VMware partners to an image profile. If you add VMware VIBs, vSphere ESXi Image Builder performs validation. If you add VIBs from two or more OEM partners simultaneously, no errors are reported but the resulting image profile might not work. Install VIBs from only one OEM vendor at a time.

If an error about acceptance level problems appears, change the acceptance level of the image profile and the acceptance level of the host. Consider carefully whether changing the host acceptance level is appropriate. VIB acceptance levels are set during VIB creation and cannot be changed.

You can add VIBs even if the resulting image profile is invalid.

Note: VMware can support only environments and configurations that are proven to be stable and fully functional through rigorous and extensive testing. Use only those supported configurations. You can use custom VIBs if you lower your host acceptance level, and as a result, supportability. In that case, track the changes you made, so you can revert them if you want to remove custom VIBs and restore the host acceptance level to the default (Partner Supporter) later. See Working with Acceptance Levels.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Run the `Get-EsxImageProfile` cmdlet to list all image profiles in all currently visible depots.

   The cmdlet returns all available profiles. You can narrow your search by using the optional arguments to filter the output.

3. Clone the profile.

   ```
   New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
   ```

   Image profiles published by VMware and its partners are read only. To make changes, you must clone the image profile. The `vendor` parameter is required.

4. Run the `Add-EsxSoftwarePackage` cmdlet to add a new package to one of the image profiles.

   ```
   Add-EsxSoftwarePackage -ImageProfile My_Profile -SoftwarePackage partner-package
   ```

   The cmdlet runs the standard validation tests on the image profile. If validation succeeds, the cmdlet returns a modified, validated image profile. If the VIB that you want to add depends on a different VIB, the cmdlet displays that information and includes the VIB that can resolve the dependency. If the acceptance level of the VIB that you want to add is lower than the image profile acceptance level, an error occurs.

Export an Image Profile to an ISO or Offline Bundle ZIP with PowerCLI Cmdlets

You can export an image profile to an ISO image or a ZIP file of component files and folders. You cannot create both by running the cmdlet once. You can use the ISO image as an ESXi installer or upload the ISO into vSphere Lifecycle Manager for upgrades.

Install the PowerCLI and all prerequisite software. See Install vSphere ESXi Image Builder and Prerequisite Software.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Run `Export-EsxImageProfile` to export the image profile.

Export Format	Cmdlet
ISO images	`Export-EsxImageProfile` with the `-ExportToIso` parameter
Offline depot ZIP files	`Export-EsxImageProfile` with the `-ExportToBundle` parameter

For the ISO image, vSphere ESXi Image Builder validates VIB signatures, adds VIB binaries to the image, and downloads the image to the specified location. For the ZIP file, vSphere ESXi Image Builder validates VIB signatures and downloads the VIB binaries to the specified location.

Exporting an Image Profile

Follow these steps to export an image profile to an ISO image.

1. Add the software depot.
   ```
   Add-EsxSoftwareDepot -DepotUrl url_or_file
   ```
2. View all available image profiles to find the name of the image profile to export.
   ```
   Get-EsxImageProfile
   ```
3. Export the image profile.
   ```
   Export-EsxImageProfile -ImageProfile "myprofile" -ExportToIso -FilePath iso_name
   ```

Follow these steps to export an image profile to a ZIP file of component files and folders.

1. Add the software depot.
   ```
   Add-EsxSoftwareDepot -DepotUrl url_or_file
   ```
2. View all available image profiles to find the name of the image profile to export.
   ```
   Get-EsxImageProfile
   ```
3. Export the image profile.
   ```
   Export-EsxImageProfile -ImageProfile "myprofile" -ExportToBundle -FilePath C:\my_bundle.zip
   ```

Use the ISO image in an ESXi installation or upload the ISO image into vSphere Lifecycle Manager to perform upgrades.

Use the ZIP file to upgrade an ESXi installation.

- Import the ZIP file into vSphere Lifecycle Manager for use with patch baselines.
- Download the ZIP file to an ESXi host or a datastore and run `esxcli software vib` commands to import the VIBs in the ZIP file.

See the *vSphere Upgrade* documentation.

Create a Custom ESXi ISO Image with PowerCLI Cmdlets

With ESXi Image Builder, you can customize an ESXi image profile, but not combine content from different depots to generate an ISO image. Starting with VMware PowerCLI 12.0, you can customize ISO images by using content from multiple software depots and a custom software specification.

Install VMware PowerCLI 12.0 or later.

Verify that you have access to the software depot that contains the software specification that you want to use.

For upgrades to ESXi 7.0 and later, the `New-IsoImage` cmdlet preserves additional metadata for ESXi 7.0.x required by the vSphere Lifecycle Manager, such as base image, addon and component. This additional metadata is not part of ISO images that you can export by using the legacy ESXi Image Builder cmdlets.

1. Gather the required information for the software specification that you use to create a custom ISO image.
   1. Get the base image version for the required patch or upgrade by running the `Get-DepotBaseImages` cmdlet:
      ```
      PS C:\> Get-DepotBaseImages -Depot C:\VMware-ESXi-7.0U2a-17867351-depot.zip
      ```
      The command output is:
      ```
      Version                                 Vendor                                  Release date
      -------                                 ------                                  ------------
      7.0.2-0.0.17867351                      VMware, Inc.                            04/29/2021 00:00:00
      ```
   2. Get other packages, such as OEM addons, with cmdlets used with new metadata in software depots. For example:
      ```
      PS C:\> Get-DepotAddons -Depot C:\addon-depot.zip
      ```

   The command output is:
   ```
   Name                    Version                 ID                      Vendor                  Release
    date
   ----                    -------                 --                      ------
    ------------
   testaddonv1             1.0.0-1                 testaddonv1:1.0.0-1     ESXLifecycle QE         02/20/2019
    18:28:23
   ```

   You can also list all components in a sofware depot with the `Get-DepotComponents` cmdlet:
   ```
   PS C:\> Get-DepotComponents -Depot C:\Intel-i40en_1.12.3.0-1OEM.700.1.0.15843807_18058526.zip
   ```

   The command output is:
   ```
   Name                            Version                         ID
            Vendor
   ----                            -------                         --
           ------
   Intel-i40en                     1.12.3.0-1OEM.700.1.0.15843807  In-
   tel-i40en:1.12.3.0-1OEM.700.1.0.15843807     Intel
   ```

   You can use any number and combination of online and offline software depots.
2. Create a software specification. For example:
   ```
   {
       "base_image": {
           "version": "7.0.2-0.0.17867351"
       },
       "add_on": {
           "name": "testaddonv1",
           "version": "1.0.0-1"
       },
       "components": {
          "Intel-i40en": "1.12.3.0-1OEM.700.1.0.15843807"
      }
   ```

```
}
```

The software specification is a JSON file that contains information about the ESXi base image and additional packages, such as a vendor add-on.

3. Generate a custom ISO image by running the `New-IsoImage` cmdlet with the parameters `Depots` ,`SoftwareSpec` and `Destination` . For example:

```
New-IsoImage -Depots "c:\temp\VMware-ESXi-7.0U1d-17551050-depot.zip" , "c:\temp\HPE-701.0.0.10.6.5.12-Jan2021-Synergy-Addon-depot.zip" -SoftwareSpec "c:\temp\HPE-70U1d-custom.JSON" -Destination "c:\temp\HPE-70U1d-custom.iso"
```

The depot(s) include the path to the zip files for the supported ESXi version and vendor add-on. The destination include the path and file name for the custom ISO file.

You can pass additional kernel options, create a live image, overwrite existing files, or check acceptance levels for individual VIBs used during the creation of the image. For more information about the `New-IsoImage` cmdlet, see https://code.vmware.com/docs/11794/cmdletreference/doc/New-IsoImage.html.

You can import the new ISO image to the vSphere Lifecycle Manager depot, so that you can create upgrade baselines, which you use for host upgrade operations.

Create a Custom PXE Image with PowerCLI Cmdlets

Starting with VMware PowerCLI 12.0, you can create a custom PXE image by using any software depot and a custom software specification.

Install VMware PowerCLI 12.0 or later.

Verify that you have access to the software depot that contains the software specification you want to use.

1. Gather the required information for the software specification that you use to create a custom PXE image.
   1. Get the base image version for the required patch or upgrade by running the `Get-DepotBaseImages` cmdlet:

```
PS C:\> Get-DepotBaseImages -Depot C:\VMware-ESXi-7.0U2a-17867351-depot.zip
```

   The command output is:

```
Version                                 Vendor                                  Release date
-------                                 ------                                  ------------
7.0.2-0.0.17867351                      VMware, Inc.                            04/29/2021 00:00:00
```

   2. Get other packages, such as OEM addons, with cmdlets used with new metadata in software depots. For example:

```
PS C:\> Get-DepotAddons -Depot C:\addon-depot.zip
```

   The command output is:

```
Name                    Version                 ID                      Vendor                  Release
 date
----                    -------                 --                      ------
 ------------
testaddonv1             1.0.0-1                 testaddonv1:1.0.0-1     ESXLifecycle QE         02/20/2019
 18:28:23
```

   You can also list all components in a sofware depot with the `Get-DepotComponents` cmdlet:

```
PS C:\> Get-DepotComponents -Depot C:\Intel-i40en_1.12.3.0-1OEM.700.1.0.15843807_18058526.zip
```

   The command output is:

```
Name                            Version                         ID
         Vendor
----                            -------                         --
        ------
Intel-i40en                     1.12.3.0-1OEM.700.1.0.15843807  In-
tel-i40en:1.12.3.0-1OEM.700.1.0.15843807     Intel
```

You can use any number and combination of online and offline software depots.

2. Create a software specification. For example:

```
{
    "base_image": {
        "version": "7.0.2-0.0.17867351"
    },
    "add_on": {
        "name": "testaddonv1",
        "version": "1.0.0-1"
    },
    "components": {
       "Intel-i40en": "1.12.3.0-1OEM.700.1.0.15843807"
   }
}
```

   The software specification is a JSON file that contains information about the ESXi base image and additional packages, such as a vendor add-on.

3. Generate a custom PXE image by running the `New-PxeImage` cmdlet with the parameters `Depots` ,`SoftwareSpec` and `Destination` . For example:

```
New-PxeImage -Depots "c:\temp\VMware-ESXi-7.0U1d-17551050-depot.zip" , "c:\temp\HPE-701.0.0.10.6.5.12-Jan2021-Synergy-Addon-depot.zip" -SoftwareSpec "c:\temp\HPE-70U1d-custom.JSON" -Destination "C:\pxe-image"
```

   The depot(s) include the path to the zip files for the supported ESXi version and vendor add-on. The destination include the path and file name for the custom PXE file.

   You can pass additional kernel options, create a live image, overwrite existing files, or check acceptance levels for individual VIBs used during the creation of the image. For more information about the `New-PxeImage` cmdlet, see https://code.vmware.com/docs/11794/cmdletreference/doc/New-PxeImage.html.

You can use the PXE image in remediation workflows of PXE booted ESXi hosts.

Preserve Image Profiles Across Sessions with PowerCLI

You can export the image profile to a ZIP file software depot and add that depot in the next session.

When you create an image profile and exit the PowerCLI session, the image profile is no longer available when you start a new session. You can export the image profile to a ZIP file software depot, and add that depot in the next session.

Install the PowerCLI and all prerequisite software. See Install vSphere ESXi Image Builder and Prerequisite Software.

1. In a PowerCLI session, create an image profile, for example by cloning an existing image profile and adding a VIB.
2. Export the image profile to a ZIP file by calling `Export-EsxImageProfile` with the `ExportToBundle` parameter.

```
Export-EsxImageProfile -ImageProfile "my_profile" -ExportToBundle -FilePath
    "C:\isos\temp-base-plus-vib25.zip"
```

3. Exit the PowerCLI session.
4. When you start a new PowerCLI session, add the depot that contains your image profile to access it.

```
Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
```

Compare Image Profiles with PowerCLI Cmdlets

You can compare two image profiles by using the `Compare-EsxImageProfile` cmdlet, for example, to see if they have the same VIB list or acceptance level . Comparing image profiles or their properties is also possible by using the PowerShell comparison operators.

Install the PowerCLI and all prerequisite software. See Install vSphere ESXi Image Builder and Prerequisite Software.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Optional: Run the `Get-EsxImageProfile` cmdlet to view a list of all image profiles in all available depots.
   In the list, you can locate the names of the image profiles you want to compare.

3. Before comparing the image profiles, assign them to variables.
   For example, you can create variables `$imageProfile1` and `$imageProfile2` to hold the names of the compared images profiles.

```
$imageProfile1
    = Get-EsxImageProfile -Name "ImageProfile1"
$imageProfile2
    = Get-EsxImageProfile -Name "ImageProfile2"
```

4. Compare the two image profiles by using the `Compare-EsxImageProfile` cmdlet or the `-eq` comparison operator, which returns a Boolean value.

   - Compare the two image profiles to get a full description of the differences by using the `Compare-EsxImageProfile` cmdlet.

```
Compare-EsxImageProfile -ReferenceProfile
      $imageProfile1 -ComparisonProfile $imageProfile2
```

   - Compare the two image profiles by VIB list and acceptance level using the `-eq` comparison operator.

```
if ($imageProfile1 -eq $imageProfile2) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

   - Compare the two image profiles by a specific property using the `-eq` comparison operator.

```
if ($imageProfile1.vendor -eq $imageProfile2.vendor) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

Compare VIBs with PowerCLI Cmdlets

You can compare two VIBs or their properties by using the PowerShell comparison operators.

Install the PowerCLI and all prerequisite software. See Install vSphere ESXi Image Builder and Prerequisite Software.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system.

Option	Action
	2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

The cmdlet returns one or more `SoftwareDepot` objects.

2. Optional: Run the `Get-EsxSoftwarePackage` cmdlet to view all available VIBs.
   In the list, you can locate the names of the VIBs you want to compare.
3. Before comparing the VIBs, assign them to variables.
   For example, you can create variables `$vib1` and `$vib2` to hold the names of the compared VIBs.

```
$vib1 = Get-EsxSoftwarePackage -Name "ReferenceVIB"
$vib2 = Get-EsxSoftwarePackage -Name "ComparisonVIB"
```

4. Use a comparison operator to compare the VIBs by contents and acceptance level or by a specific property.
   - Compare the two VIBs by their contents and acceptance level.

```
if ($vib1 -eq $vib2) {
   Write-host "Successfully verified that both VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

   - Compare a specific property of the VIBs by using a comparison operator such as `-eq`, `-lt`, `-le`, `-gt`, or `-ge`.

```
if ($vib1.VersionObject -lt $vib2.VersionObject) {
   Write-host "Successfully verified that both the VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

Working with Acceptance Levels

Hosts, image profiles, and individual VIBs have acceptance levels. VIB acceptance levels show how the VIB was tested. Understanding what each acceptance level implies, how to change levels, and what a change implies is an important part of installation and update procedures.

Acceptance levels are set for hosts, image profiles, and individual VIBs. The default acceptance level for an ESXi image or image profile is PartnerSupported.

Host acceptance levels

The host acceptance level determines which VIBs you can install on a host. You can change a host's acceptance level with ESXCLI commands. By default, ESXi hosts have an acceptance level of PartnerSupported to allow for easy updates with PartnerSupported VIBs.

Note: VMware supports hosts at the PartnerSupported acceptance level. For problems with individual VIBs with PartnerSupported acceptance level, contact your partner's support organization.

Image profile acceptance levels

The image profile acceptance level is set to the lowest VIB acceptance level in the image profile. If you want to add a VIB with a low acceptance level to an image profile, you can change the image profile acceptance level with the `Set-EsxImageProfile` cmdlet. See Set the Image Profile Acceptance Level.

The vSphere Lifecycle Manager does not display the actual acceptance level. Use vSphere ESXi Image Builder cmdlets to retrieve the acceptance level information for VIBs and image profiles.

VIB acceptance levels	A VIB's acceptance level is set when the VIB is created. Only the VIB creator can set the acceptance level.

If you attempt to provision a host with an image profile or VIB that has a lower acceptance level than the host, an error occurs. Change the acceptance level of the host to install the image profile or VIB. See Change the Host Acceptance Level. Changing the acceptance level of the host changes the support level for that host.

The acceptance level of a host, image profile, or VIB lets you determine who tested the VIB and who supports the VIB. VMware supports the following acceptance levels .

VMwareCertified	The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only I/O Vendor Program (IOVP) program drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.
VMwareAccepted	VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plug-ins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
PartnerSupported	VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
CommunitySupported	The CommunitySupported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs. VIBs at this level have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

Change the Host Acceptance Level

You can lower the host acceptance level to match the acceptance level for a VIB or image profile you want to install.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

The acceptance level of each VIB on a host must be at least as high as the acceptance level of the host. For example, you cannot install a VIB with PartnerSupported acceptance level on a host with VMwareAccepted acceptance level. You must first lower the acceptance level of the host. For more information on acceptance levels, see Acceptance Levels.

Warning: Changing the host acceptance level to CommunitySupported affects the supportability of your host and might affect the security of your host.

1. Retrieve the acceptance level for the VIB or image profile.

Option	Description
View information for all VIBs	`esxcli --server=server_name software sources vib list --depot=depot_URL`
View information for a specified VIB	`esxcli --server=server_name software sources vib list --viburl=vib_URL`
View information for all image profiles	`esxcli --server=server_name software sources profile list --depot=depot_URL`
View information for a specified image profile	`esxcli --server=server_name software`

Option	Description
	`sources profile get --depot=depot_URL --profile=profile_name`

2. View the host acceptance level.
   ```
   esxcli --server=server_name software acceptance get
   ```
3. Change the acceptance level of the host.
   ```
   esxcli
       --server=server_name software acceptance set --level=acceptance_level
   ```
   The value for *acceptance_level* can be `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. The values for *acceptance_level* are case-sensitive.

   Note: If the host has a higher acceptance level than the VIB or image profile you want to add, you can run commands in the `esxcli software vib` or `esxcli software profile` namespace with the --force option. When you use the --force option, a warning appears because you enforce a VIB or image profile with lower acceptance level than the acceptance level of the host and your setup is no longer consistent. The warning is repeated when you install VIBs, remove VIBs, or perform certain other operations on the host that has inconsistent acceptance levels.

Set the Image Profile Acceptance Level

If you want to add a VIB to an image profile, and the acceptance level of the VIB is lower than that of the image profile, you can clone the image profile with a lower acceptance level or change the image profile's acceptance level.

Install PowerCLI and all prerequisite software. See Install vSphere ESXi Image Builder and Prerequisite Software.

You can specify VMwareCertified, VMwareAccepted, PartnerSupported, or CommunitySupported as an acceptance level of an image profile. If you lower the acceptance level, the level of support for the image profile and hosts that you provision with it changes. For more information, see Acceptance Levels.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.
2. Get the acceptance level for the image profile.
   ```
   Get-EsxImageProfile -Name string
   ```
3. Set the acceptance level of the image profile.
   ```
   Set-EsxImageProfile -Name string -AcceptanceLevel level
   ```

vSphere ESXi Image Builder Workflows with PowerCLI Cmdlets

vSphere ESXi Image Builder workflows are examples for cmdlet use and do not represent actual tasks.

vSphere ESXi Image Builder workflows are examples for cmdlet use. Workflows do not represent actual tasks, but illustrate how you might explore different ways of using a cmdlet. Administrators trying out the workflows benefit from some experience with PowerCLI, Microsoft PowerShell, or both.

Examine Depot Contents

You can examine software depots and VIBs with vSphere ESXi Image Builder cmdlets. You can use wildcards to examine depot contents. All wildcard expressions are supported.

Verify that PowerCLI and prerequisite software is installed. See Install vSphere ESXi Image Builder and Prerequisite Software.

The workflow itself passes parameters by name. However, you can pass parameters as objects by accessing variables.

You can use filtering options and wildcard expressions to examine depot contents.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Retrieve image profiles.

   You can filter by vendor, name, and acceptance level.

   - `Get-EsxImageProfiles`

     Returns an array of `ImageProfile` objects from all depots you added to the session.
   - `Get-EsxImageProfile -Vendor "C*"`

     Returns all image profiles created by a vendor with a name that starts with the letter C.

3. Retrieve software packages by using the `Get-EsxSoftwarePackage` cmdlet.

   You can filter, for example by vendor or version, and you can use the standard PowerShell wildcard characters.

   - `Get-EsxSoftwarePackage -Vendor "V*"`

     Returns all software packages from a vendor with a name that starts with the letter V.
   - `Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"`

     Returns all software packages with a name that contains the string `scsi` in it from a vendor with a name that starts with the letter V.
   - `Get-EsxSoftwarePackage -Version "2.0*"`

     Returns all software packages with a version string that starts with 2.0.

4. Use `-Newest` to find the latest package.

   - `Get-EsxSoftwarePackage -Vendor "V*" -Newest`

     Returns the newest package for the vendors with a name that starts with the letter V, and displays the information as a table.
   - `Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list`

     Returns detailed information about each software package by using a pipeline to link the output of the request for software packages to the PowerShell `format-list` cmdlet.

5. View the list of VIBs in the image profile.

   ```
   (Get-EsxImageProfile -Name "Robin's Profile").VibList
   ```

   `VibList` is a property of the `ImageProfile` object.

6. Retrieve software packages released before or after a certain date by using the `CreatedBefore` or `CreatedAfter` parameter.

```
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Depot Content Examination Using Variables

This workflow example examines depot contents by passing in parameters as objects accessed by position in a variable, instead of passing in parameters by name. You can run the following commands in sequence from the PowerCLI prompt. Replace names with names that are appropriate in your installation.

```
Get-EsxSoftwarePackage -Vendor "V*"
Get-EsxSoftwarePackage -Vendor "V*" -Name "r*"
Get-EsxSoftwarePackage -Version "2.0*"
$ip1 = Get-EsxImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Create Image Profiles by Cloning Workflow

You can use vSphere ESXi Image Builder cmdlets to check which depots are available, to add a depot, to view image profile information, and to create a new image profile by cloning one of the available image profiles.

Verify that PowerCLI and prerequisite software is installed. See Install vSphere ESXi Image Builder and Prerequisite Software.

Published profiles are usually read-only and cannot be modified. Even if a published profile is not read-only, cloning instead of modifying the profile is a best practice, because modifying the original profile erases the original. You cannot revert to the original, unmodified profile except by reconnecting to a depot.

A profile cloning workflow might include checking the current state of the system, adding a software depot, and cloning the profile.

1. In a PowerShell window, check whether any software depots are defined for the current session.

```
$DefaultSoftwareDepots
```

   PowerShell returns the currently defined depots, or nothing if you just started PowerShell.

2. If the depot containing the profile that you want to clone does not appear in the results, add it to the current session.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl` *`depot_url`*`.`
ZIP file	1. Download the ZIP file to a local file path. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\file_path\`*`offline-bundle`*`.zip`

   PowerShell adds the specified depot to your current session and lists all current depots.

3. Optional: Check the `$DefaultSoftwareDepots` variable, which now returns the newly added depot.
4. View all available image profiles.

```
Get-EsxImageProfile
```

5. To clone an image profile, enter its name, a new name for the new profile, and a name of the vendor.

```
$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor "Vendor20"
```

6. Optional: View the newly created image profile, `$ip` .

   PowerShell returns the information about the image profile in tabular format.

```
Name                Vendor          Last Modified          Acceptance Level
----                ------          -------------          ----------------
Test Profile 42     Vendor20        9/15/2010 5:45:43...   PartnerSupported
```

Creating Image Profile by Cloning Using Variables

This workflow example repeats the steps of this workflow by passing in parameters as objects accessed by position in a variable, instead of passing in parameters by name. You can run the following cmdlets in sequence from the PowerCLI prompt.

```
$DefaultSoftwareDepots
Add-EsxSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-EsxImageProfile
$profs
$ip = New-EsxImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Create New Image Profiles Workflow

In most situations, you create an image profile by cloning an existing profile. Some VMware customers or partners might need to create a new image profile. Pay careful attention to dependencies and acceptance levels if you create an image profile from scratch.

- PowerCLI and prerequisite software is installed. See Install vSphere ESXi Image Builder and Prerequisite Software.
- You have access to a depot that includes a base image and one or more VIBs. VMware and VMware partners have public depots, accessible by a URL. VMware or VMware partners can create a ZIP file that you can unzip to your local environment and access by using a file path.

The system expects that the acceptance level of the VIBs you add to the base image is at least as high as the level of the base image. If you have to add a VIB with a lower acceptance level to the image profile, you must lower the image profile acceptance level. For more information, see Set the Image Profile Acceptance Level.

As an alternative to specifying the parameters on the command line, you can use the PowerShell prompting mechanism to specify string parameters. Prompting does not work for other parameters such as objects.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Run the `Get-EsxImageProfile` cmdlet to list all image profiles in all currently visible depots. You can narrow your search by using the optional arguments to filter the output.

   ```
   Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
   ```

3. Create a new profile, assign it a name and vendor, and add a base package.

   ```
   New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-base[0],esx-xlibs[0]
   ```

   The example uses the esx-base package. In most cases, you include the esx-base package when you create a new image profile. Names that contain spaces are surrounded by quotes.

4. Use a pipeline to pass the new image profile to `format-list` for detailed information about the new package.

   ```
   (Get-EsxImageProfile -Name "Test #2").VibList | format-list
   ```

Creating Image Profiles from Scratch Using Variables

This command sequence repeats the steps of the workflow, but passes parameters as objects, accessed by position in a variable, instead of passing parameters by name. You can run the following commands in sequence at the PowerCLI prompt.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage $pkgs[0]
$ip2.VibList | format-list
```

Edit Image Profiles Workflow

You can create a custom image by cloning and editing an image profile by using PowerCLI. You can add or remove one or more VIBs in the existing profile. If adding or removing VIBs prevents the image profile from working correctly, an error occurs.

- PowerCLI and prerequisite software is installed. See Install vSphere ESXi Image Builder and Prerequisite Software.
- You have access to a depot that includes a base image and one or more VIBs. VMware and VMware partners make public depots, accessible by a URL, available. VMware or VMware partners can create a ZIP file that you can download to your local environment and access by using a file path.

1. In a PowerCLI session, run the `Add-EsxSoftwareDepot` cmdlet for each depot you want to work with.

Option	Action
Remote depot	Run `Add-EsxSoftwareDepot -DepotUrl <depot_url>`.
ZIP file	1. Download the ZIP file to a local file system. 2. Run `Add-EsxSoftwareDepot -DepotUrl C:\<file_path>\<offline-bundle>.zip`

   The cmdlet returns one or more `SoftwareDepot` objects.

2. Use a pipeline to pass the image profile you intend to edit to `format-list` to see detailed information.
   In this example, the image profile created in Create New Image Profiles Workflow contains only the base image. A newly created image profile is not included in the depot. Instead, you access the image profile by name or by binding it to a variable.

   ```
   Get-EsxImageProfile "Test #2" | format-list
   ```

   PowerShell returns the information.

   ```
   Name            : Test #2
   Vendor        : Vendor42
   ...
   VibList       : {esx-base 5.0.0.-...,}
   ```

3. Optional: If you are adding a VIB with a lower acceptance level than that of the image profile, change the acceptance level of the image profile.

   ```
   Set-EsxImageProfile -ImageProfile "Test #2" -AcceptanceLevel VMwareAccepted
   ```

   PowerShell returns the information about the changed profile in tabular format.

   ```
   Name           Vendor           Last Modified       Acceptance Level
   ----           ------           -------------       ----------------
   Test #2        Vendor42         9/22/2010 12:05:... VMwareAccepted
   ```

4. Add a software package (VIB) to the image profile. You can add the package by name.

   ```
   Add-EsxSoftwarePackage -ImageProfile "Test #2"
   ```

```
-SoftwarePackage NewPack3
```

PowerShell returns the information about the image profile in tabular format.

```
Name           Vendor          Last Modified       Acceptance Level
----           ------          -------------       ----------------
Test #2        Vendor42        9/22/2010 12:05:... VMwareAccepted
```

Note: If an error occurs when you add the software package, you might have a problem with acceptance levels, see Working with Acceptance Levels

5. View the image profile again.

```
Get-EsxImageProfile "Test #2" | format-list
```

The VIB list is updated to include the new software package and the information is displayed.

```
Name            : Test #2
Vendor        : Vendor42
...
VibList       : {esx-base 5.0.0.-..., NewPack3}
```

Editing Image Profiles by Using Variables

This cmdlet sequence repeats the steps of the workflow but passes parameters as objects, accessed by position in a variable, instead of passing parameters by name. You can run the following cmdlets in sequence from the PowerCLI prompt.

```
Add-EsxSoftwareDepot -DepotUrl depot_url
$ip2 = Get-EsxImageProfile -name "Test #2"
$ip2 | format-list
Set-EsxImageProfile -ImageProfile $ip2 -AcceptanceLevel VMwareAccepted
Add-EsxImageSoftwarePackage -ImageProfile $ip2 -SoftwarePackage NewPack3
$ip2 | format-list
```

Required Information for ESXi Installation

Interactive installation prompts you for the required system information, but you must supply this information in the installation script.

In an interactive installation, the system prompts you for the required system information. In a scripted installation, you must supply this information in the installation script. For future use, note the values you use during the installation. These notes are useful if you must reinstall ESXi and reenter the values that you originally selected.

Table 11: Required Information for ESXi Installation

Information	Required or Optional	Default	Comments
Keyboard layout	Required	U.S. English	
VLAN ID	Optional	None	Range: 0 through 4094
IP address	Optional	DHCP	You can allow DHCP to configure the network during installation. After installation, you can change the network settings.
Subnet mask	Optional	Calculated based on the IP address	
Gateway	Optional	Based on the configured IP address and subnet mask	

Information	Required or Optional	Default	Comments
Primary DNS	Optional	Based on the configured IP address and subnet mask	
Secondary DNS	Optional	None	
Host name	Required for static IP settings	None	The vSphere Client can use either the host name or the IP address to access the ESXi host.
Install location	Required	None	Must be at least 5 GB if you install the components on a single disk.
Root password	Required	None	The root password must contain between 8 and 40 characters. For information about passwords see the *vSphere Security* documentation.

Installing ESXi

You can install ESXi interactively, with a scripted installation, or with vSphere Auto Deploy.

- Installing ESXi Interactively
- Installing or Upgrading Hosts by Using a Script
- Overview of the Network Boot Installation Process
- Installing ESXi Using vSphere Auto Deploy

Installing ESXi Interactively

Use the interactive installation option for small deployments of fewer than five hosts.

In a typical interactive installation, you boot the ESXi installer and respond to the installer prompts to install ESXi to the local host disk. The installer reformats and partitions the target disk and installs the ESXi boot image. If you have not installed ESXi on the target disk before, all data on the drive is overwritten, including hardware vendor partitions, operating system partitions, and associated data.

Note: To ensure that you do not lose any data, migrate the data to another machine before you install ESXi.

If you are installing ESXi on a disk that contains a previous installation of ESXi or ESX, or a VMFS datastore, the installer provides you with options for upgrading. See the *vSphere Upgrade* documentation.

Install ESXi Interactively

You use the ESXi CD/DVD or a USB flash drive to install the ESXi software onto a SAS, SATA, SCSI hard drive, or USB drive.

- You must have the ESXi installer ISO in one of the following locations:
  - On CD or DVD. If you do not have the installation CD/DVD, you can create one. See Download and Burn the ESXi Installer ISO Image to a CD or DVD
  - On a USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade.

  Note: You can also PXE boot the ESXi installer to run an interactive installation or a scripted installation. See Network Booting the ESXi Installer.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- Verify that a keyboard and monitor are attached to the machine on which the ESXi software is installed. Alternatively, use a remote management application. See Using Remote Management Applications.

- Consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. When you disconnect network storage, any files on the disconnected disks are unavailable at installation.
  Do not disconnect a LUN that contains an existing ESX or ESXi installation. Do not disconnect a VMFS datastore that contains the Service Console of an existing ESX installation. These actions can affect the outcome of the installation.
- Gather the information required by the ESXi installation wizard. See Required Information for ESXi Installation.
- Verify that ESXi Embedded is not present on the host machine. ESXi Installable and ESXi Embedded cannot exist on the same host.

1. Insert the ESXi installer CD/DVD into the CD/DVD-ROM drive, or attach the Installer USB flash drive and restart the machine.
2. Set the BIOS to boot from the CD-ROM device or the USB flash drive.
   See your hardware vendor documentation for information on changing boot order.
3. On the Select a Disk page, select the drive on which to install ESXi, and press Enter.
   Press F1 for information about the selected disk.

   Note: Do not rely on the disk order in the list to select a disk. The disk order is determined by the BIOS and might be out of order. This might occur on systems where drives are continuously being added and removed.

   If you select a disk that contains data, the Confirm Disk Selection page appears.

   If you are installing on a disc with a previous ESXi or ESX installation or VMFS datastore, the installer provides several choices.

   Important: If you are upgrading or migrating an existing ESXi installation, see the *VMware ESXi Upgrade* documentation.

   If you select a disk that is in vSAN disk group, the resulting installation depends on the type of disk and the group size:

   - If you select an SSD, the SSD and all underlying HDDs in the same disk group are wiped.
   - If you select an HDD, and the disk group size is greater than two, only the selected HDD is wiped.
   - If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD is wiped.

   For more information about managing vSAN disk groups, see the *vSphere Storage* documentation.
4. Select the keyboard type for the host.
   You can change the keyboard type after installation in the direct console.
5. Enter the root password for the host.
   You can change the password after installation in the direct console.
6. Press Enter to start the installation.
7. When the installation is complete, remove the installation CD, DVD, or USB flash drive.
8. Press Enter to reboot the host.
9. Set the first boot device to be the drive on which you installed ESXi in step 5.
   For information about changing boot order, see your hardware vendor documentation.

   Note: UEFI systems might require additional steps to set the boot device. See Host Fails to Boot After You Install ESXi in UEFI Mode

After the installation is complete, you can migrate existing VMFS data to the ESXi host.

You can boot a single machine from each ESXi image. Booting multiple devices from a single shared ESXi image is not supported.

Set up basic administration and network configuration for ESXi. See After You Install and Set Up ESXi.

Install ESXi on a Software iSCSI Disk

When you install ESXi to a software iSCSI disk, you must configure the target iSCSI qualified name (IQN).

- Verify that the target IQN is configured in the iBFT BIOS target parameter setting. This setting is in the option ROM of the network interface card (NIC) to be used for the iSCSI LUN. See the vendor documentation for your system.
- Deactivate the iBFT adapter option to boot to the iSCSI target. This action is necessary to make sure that the ESXi installer boots, rather than the iSCSI target. When you start your system, follow the prompt to log in to your iBFT adapter and deactivate the option to boot to the iSCSI target. See the vendor documentation for your system and iBFT adapter. After you finish the ESXi installation, you can reenable the option to boot from the LUN you install ESXi on.

During system boot, the system performs a Power-On Self Test (POST), and begins booting the adapters in the order specified in the system BIOS. When the boot order comes to the iSCSI Boot Firmware Table (iBFT) adapter, the adapter attempts to connect to the target, but does not boot from it. See Prerequisites.

If the connection to the iSCSI target is successful, the iSCSI boot firmware saves the iSCSI boot configuration in the iBFT. The next adapter to boot must be the ESXi installation media, either a mounted ISO image or a physical CD-ROM.

1. Start an interactive installation from the ESXi installation CD/DVD or mounted ISO image.
2. On the Select a Disk screen, select the iSCSI target you specified in the iBFT BIOS target parameter setting.

   If the target does not appear in this menu, make sure that the TCP/IP and initiator iSCSI IQN settings are correct. Check the network Access Control List (ACL) and confirm that the adapter has adequate permissions to access the target.
3. Follow the prompts to complete the installation.
4. Reboot the host.
5. In the host BIOS settings, enter the iBFT adapter BIOS configuration, and change the adapter parameter to boot from the iSCSI target.

   See the vendor documentation for your system.

On your iBFT adapter, reenable the option to boot to the iSCSI target, so the system will boot from the LUN you installed ESXi on.

Installing or Upgrading Hosts by Using a Script

You can quickly deploy hosts by using scripted, unattended installations or upgrades.

Scripted installations or upgrades provide an efficient way to deploy multiple hosts. The installation or upgrade script contains the installation settings for . You can apply the script to all hosts that you want to have a similar configuration.

For a scripted installation or upgrade, you must use the supported commands to create a script. You can edit the script to change settings that are unique for each host.

The installation or upgrade script can reside in one of the following locations:

- FTP server
- HTTP/HTTPS server
- NFS server
- USB flash drive
- CD-ROM drive

Approaches for Scripted Installation

You can install ESXi on multiple machines using a single script for all of them or a separate script for each machine.

For example, because disk names vary from machine to machine, one of the settings that you might want to configure in a script is the selection for the disk to install ESXi on.

Table 12: Scripted Installation Choices

Option	Action
Always install on the first disk on multiple machines.	Create one script.
Install ESXi on a different disk for each machine.	Create multiple scripts.

For information about the commands required to specify the disk to install on, see Installation and Upgrade Script Commands.

Enter Boot Options to Run an Installation or Upgrade Script

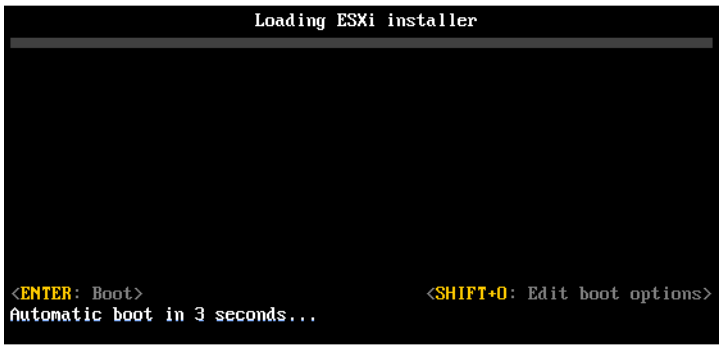
You can start an installation or upgrade script by typing boot options at the ESXi installer boot command line.

At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See About the boot.cfg File and Network Booting the ESXi Installer.

To specify the location of the installation script, set the `ks=filepath` option, where *`filepath`* indicates the location of your kickstart file. Otherwise, a scripted installation or upgrade cannot start. If `ks=filepath` is omitted, the text installer is run.

Supported boot options are listed in Boot Options .

1. Start the host.
2. When the ESXi installer window appears, press Shift+O to edit boot options.



3. At the `runweasel` command prompt, type `ks=`*`location of installation script plus boot command-line options`*.

   Boot Option

   You type the following boot options:

   ```
   ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000 net-
   mask=255.255.255.0 gateway=00.00.00.000
   ```

Boot Options

When you perform a scripted installation, you might need to specify options at boot time to access the kickstart file.

Supported Boot Options

Table 13: Boot Options for ESXi Installation

Boot Option	Description
`BOOTIF=`*`hwtype-MAC address`*	Similar to the `netdevice` option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the `syslinux.org` site.
`gateway=`*`ip address`*	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
`ip=`*`ip address`*	Sets up a static IP address to be used for downloading the installation script and the installation media. Note: the PXELINUX format for this option is also supported. See the IPAPPEND option under SYSLINUX at the `syslinux.org` site.
`ks=cdrom:/`*`path`*	Performs a scripted installation with the script at *`path`*, which resides on the CD in the CD-ROM drive. Each CDROM is mounted and checked until the file that matches the path is found. **Important:** If you have created an installer ISO image with a custom installation or upgrade script, you must use uppercase characters to provide the path of the script, for example, `ks=cdrom:/KS_CUST.CFG` .
`ks=file://`*`path`*	Performs a scripted installation with the script at *`path`*.
`ks=`*`protocol`*`://`*`serverpath`*	Performs a scripted installation with a script located on the network at the given URL. *`protocol`* can be `http`, `https`, `ftp`, or `nfs`. An example using NFS protocol is `ks=nfs://`*`host`*`/`*`porturl-path`* . The format of an NFS URL is specified in RFC 2224.
`ks=usb`	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named `ks.cfg`. The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the `ks.cfg` file is found. Only FAT16 and FAT32 file systems are supported.
`ks=usb:/`*`path`*	Performs a scripted installation with the script file at the specified path, which resides on USB.
`ksdevice=`*`device`*	Tries to use a network adapter *`device`* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`nameserver=`*`ip address`*	Specifies a domain name server to be used for downloading the installation script and installation media.

Boot Option	Description
`netdevice=device`	Tries to use a network adapter *`device`* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`netmask=subnet mask`	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
`vlanid=vlanid`	Configure the network card to be on the specified VLAN.
`systemMediaSize=small`	Limits the size of system storage partitions on the boot media. The selected value must fit the purpose of your system. You can select from the following values: • *`min`* (32 GB, for single disk or embedded servers) • *`small`* (64 GB, for servers with at least 512 GB RAM) • *`default`* (128 GB) • *`max`* (consume all available space, for multi-terabyte servers)

For more information on ESXi booting options post installation, see VMware knowledge base article 77009.

About Installation and Upgrade Scripts

The installation/upgrade script is a text file, for example `ks.cfg`, that contains supported commands.

The command section of the script contains the ESXi installation options. This section is required and must appear first in the script.

About the Default ks.cfg Installation Script

The ESXi installer includes a default installation script that performs a standard installation to the first detected disk.

The default `ks.cfg` installation script is located in the initial RAM disk at `/etc/vmware/weasel/ks.cfg`. You can specify the location of the default `ks.cfg` file with the `ks=file://etc/vmware/weasel/ks.cfg` boot option. See Enter Boot Options to Run an Installation or Upgrade Script.

When you install ESXi using the `ks.cfg` script, the default root password is `myp@ssw0rd` .

You cannot modify the default script on the installation media. After the installation, you can use the vSphere Client to log in to the vCenter Server that manages the ESXi host and modify the default settings.

The default script contains the following commands:

```
#
# Sample scripted installation file
#

# Accept the VMware End User License Agreement
vmaccepteula

# Set the root password for the DCUI and Tech Support Mode
rootpw myp@ssw0rd

# Install on the first local disk available on machine
```

```
install --firstdisk --overwritevmfs

# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0

# A sample post-install script
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

Locations Supported for Installation or Upgrade Scripts

In scripted installations and upgrades, the ESXi installer can access the installation or upgrade script, also called the kickstart file, from several locations.

The following locations are supported for the installation or upgrade script:

- CD/DVD. See Create an Installer ISO Image with a Custom Installation or Upgrade Script.
- USB Flash drive. See Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script.
- A network location accessible through the following protocols: NFS, HTTP, HTTPS, FTP

Path to the Installation or Upgrade Script

You can specify the path to an installation or upgrade script.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` is the path to the ESXi installation script, where*XXX.XXX.XXX.XXX*is the IP address of the machine where the script resides. See About Installation and Upgrade Scripts.

To start an installation script from an interactive installation, you enter the ks= option manually. See Enter Boot Options to Run an Installation or Upgrade Script.

Installation and Upgrade Script Commands

To modify the default installation or upgrade script or to create your own script, use supported commands. Use supported commands in the installation script, which you specify with a boot command when you boot the installer.

To determine which disk to install or upgrade ESXi on, the installation script requires one of the following commands: `install`, `upgrade`, or `installorupgrade`. The `install` command creates the default partitions, including a VMFS datastore that occupies all available space after the other partitions are created.

accepteula or vmaccepteula (Required)

Accepts the ESXi license agreement.

clearpart (Optional)

Clears any existing partitions on the disk. Requires the `install` command to be specified. Carefully edit the `clearpart` command in your existing scripts.

--drives=

Remove partitions on the specified drives.

--alldrives

Ignores the `--drives=` requirement and allows clearing of partitions on every drive.

--ignoredrives=

Removes partitions on all drives except those specified. Required unless the `--drives=` or `--alldrives` flag is specified.

--overwritevmfs

Allows overwriting of VMFS partitions on the specified drives. By default, overwriting VMFS partitions is not allowed.

--firstdisk=
disk-type1
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESXi installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

dryrun (Optional)

Parses and checks the installation script. Does not perform the installation.

install

Specifies that this is a fresh installation. Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*`diskname`* , the *`diskname`* can be a disk name or a full disk filesystem path in ESXi, for example:

- Disk name: `--disk=naa.6d09466044143600247aee55ca2a6405` or
- Device path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

For accepted disk name formats, see Disk Device Names.

--firstdisk=
***disk-type1*,**
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather

than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

--ignoressd

Excludes solid-state disks from eligibility for partitioning. This option can be used with the `install` command and the --firstdisk option. This option takes precedence over the --firstdisk option. This option is invalid with the --drive or --disk options and with the `upgrade` and `installorupgrade` commands. See the *vSphere Storage* documentation for more information about preventing SSD formatting during auto-partitioning.

--overwritevsan

You must use the --overwritevsan option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a vSAN disk group. If you use this option and no vSAN partition is on the selected disk, the installation fails. When you install ESXi on a disk that is in vSAN disk group, the result depends on the disk that you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group is wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD is wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD is wiped.

For more information about managing vSAN disk groups, see the *vSphere Storage* documentation.

--overwritevmfs

Required to overwrite an existing VMFS datastore on the disk before installation.

--preservevmfs

Preserves an existing VMFS datastore on the disk during installation.

--novmfsondisk

Prevents a VMFS partition from being created on this disk. Must be used with --overwritevmfs if a VMFS partition exists on the disk.

installorupgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*`diskname`* , the *`diskname`* can be a disk name or a full disk filesystem path in ESXi, for example:

- Disk name: `--disk=naa.6d09466044143600247aee55ca2a6405` or
- Device path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

For accepted disk name formats, see Disk Device Names.

--firstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather

than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

--overwritevsan

You must use the --overwritevsan option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a vSAN disk group. If you use this option and no vSAN partition is on the selected disk, the installation fails. When you install ESXi on a disk that is in a vSAN disk group, the result depends on the disk that you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group is wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD is wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD is wiped.

For more information about managing vSAN disk groups, see the *vSphere Storage* documentation.

--overwritevmfs

Install ESXi if a VMFS partition exists on the disk, but no ESX or ESXi installation exists. Unless this option is present, the installer fails if a VMFS partition exists on the disk, but an ESX or ESXi installation is missing.

keyboard (Optional)

Sets the keyboard type for the system.

keyboardType

Specifies the keyboard map for the selected keyboard type. *keyboardType* must be one of the following types.

- Belgian
- Brazilian
- Croatian
- Czechoslovakian
- Danish
- Estonian
- Finnish
- French
- German
- Greek
- Icelandic
- Italian
- Japanese
- Latin American
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss German
- Turkish
- Ukrainian
- United Kingdom
- US Default

- US Dvorak

serialnum or vmserialnum (Optional)

The command is supported in ESXi version 5.1 and later. Configures licensing. If not included, ESXi installs in evaluation mode.

--esx=<license-key>

Specifies the vSphere license key to use. The format is 5 five-character groups (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (Optional)

Specifies a network address for the system.

--bootproto=[dhcp|static]

Specifies whether to obtain the network settings from DHCP or set them manually.

--device=

Specifies either the MAC address of the network card or the device name, in the form `vmnicNN` , as in `vmnic0` . This option refers to the uplink device for the virtual switch.

--ip=

Sets an IP address for the machine to be installed, in the form `xxx.xxx.xxx.xxx` . Required with the --bootproto=static option and ignored otherwise.

--gateway=

Designates the default gateway as an IP address, in the form `xxx.xxx.xxx.xxx` . Used with the --bootproto=static option.

--nameserver=

Designates the primary name server as an IP address. Used with the `--bootproto=static` option. Omit this option if you do not intend to use DNS.

The `--nameserver` option can accept two IP addresses. For example: `--nameserver="10.126.87.104[,10.126.87.120]"`

--netmask=

Specifies the subnet mask for the installed system, in the form `255.xxx.xxx.xxx` . Used with the `--bootproto=static` option.

--hostname=

Specifies the host name for the installed system.

--vlanid= ***vlanid***

Specifies which VLAN the system is on. Used with either the --bootproto=dhcp or `--bootproto=static` option. Set to an integer from 1 to 4096.

--addvmportgroup=(0|1)

Specifies whether to add the VM Network port group, which is used by virtual machines. The default value is 1.

paranoid (Optional)

Causes warning messages to interrupt the installation. If you omit this command, warning messages are logged.

part or partition (Optional)

Creates an extra VMFS datastore on the system. Only one datastore per disk can be created. Cannot be used on the same disk as the `install` command. Only one partition can be specified per disk and it can only be a VMFS partition.

datastore name

Specifies where the partition is to be mounted.

--ondisk= or --ondrive=

Specifies the disk or drive where the partition is created.

--onfirstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --onfirstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

reboot (Optional)

Reboots the machine after the scripted installation is complete.

<--noeject>

The CD is not ejected after the installation.

rootpw (Required)

Sets the root password for the system.

--iscrypted

Specifies that the password is encrypted.

password

Specifies the password value.

upgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*`diskname`* , the *`diskname`* can be a disk name or a full disk filesystem path in ESXi, for example:

- Disk name: `--disk=naa.6d09466044143600247aee55ca2a6405` or
- Device path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

For accepted disk name formats, see Disk Device Names.

--firstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

%include or include (Optional)

Specifies another installation script to parse. This command is treated similarly to a multiline command, but takes only one argument.

filename

For example: `%include part.cfg`

%pre (Optional)

Specifies a script to run before the kickstart configuration is evaluated. For example, you can use it to generate files for the kickstart file to include.

--interpreter
=[python|busybox]

Specifies an interpreter to use. The default is busybox.

%post (Optional)

Runs the specified script after package installation is complete. If you specify multiple `%post` sections, they run in the order that they appear in the installation script.

--interpreter
=[python|busybox]

Specifies an interpreter to use. The default is busybox.

--timeout=secs

Specifies a timeout for running the script. If the script is not finished when the timeout expires, the script is forcefully stopped.

--ignorefailure
=[true|false]

If true, the installation is considered a success even if the `%post` script stops with an error.

%firstboot

Creates an `init` script that runs only during the first boot. The script has no effect on subsequent boots. If multiple `%firstboot` sections are specified, they run in the order that they appear in the kickstart file.

Note: You cannot check the semantics of `%firstboot` scripts until the system is booting for the first time. A `%firstboot` script might contain potentially catastrophic errors that are not exposed until after the installation is complete.

Important: The `%firstboot` script does not run, if secure boot is enabled on the ESXi host.

--interpreter
=[python|busybox]

Specifies an interpreter to use. The default is busybox.

Note: You cannot check the semantics of the `%firstboot` script until the system boots for the first time. If the script contains errors, they are not exposed until after the installation is complete.

Disk Device Names

The `install`, `upgrade`, and `installorupgrade` installation script commands require the use of disk device names.

Table 14: Disk Device Names

Format	Example	Description
NAA	naa.6d09466044143600247aee55ca2a6405	SCSI INQUIRY identifier
EUI	eui.3966623838646463	SCSI INQUIRY identifier
T10	t10.SanDisk00Cruzer_Blade000000004C5300011711 18101244	SCSI INQUIRY identifier
VML	vml.00025261	Legacy VMkernel identifier
MPX	mpx.vmhba0:C0:T0:L0	Path-based identifier

For more information on storage device names, see *Storage Device Names and Identifiers* in the *vSphere Storage* documentation.

About the boot.cfg File

The boot loader configuration file `boot.cfg` specifies the kernel, the kernel options, and the boot modules that the `mboot.c32` or `mboot.efi` boot loader uses in an ESXi installation.

The `boot.cfg` file is provided in the ESXi installer. You can modify the kernelopt line of the `boot.cfg` file to specify the location of an installation script or to pass other boot options.

The `boot.cfg` file has the following syntax:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
prefix=DIRPATH
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1---FILEPATH2... ---FILEPATHn

# Any other line must remain unchanged.
```

The commands in `boot.cfg` configure the boot loader.

Table 15: Commands in boot.cfg.

Command	Description
`title=`*`STRING`*	Sets the boot loader title to *`STRING`*.
`prefix=`*`STRING`*	(Optional) Adds *`DIRPATH/`* in front of every *`FILEPATH`* in the `kernel=` and `modules=` commands that do not already start with / or with `http://`.
`kernel=`*`FILEPATH`*	Sets the kernel path to *`FILEPATH`*.
`kernelopt=`*`STRING`*	Appends *`STRING`* to the kernel boot options.
`modules=`*`FILEPATH1 --- FILEPATH2... --- FILEPATHn`*	Lists the modules to be loaded, separated by three hyphens (`---`).

See Create an Installer ISO Image with a Custom Installation or Upgrade Script and Network Booting the ESXi Installer.

Install or Upgrade ESXi from a CD or DVD by Using a Script

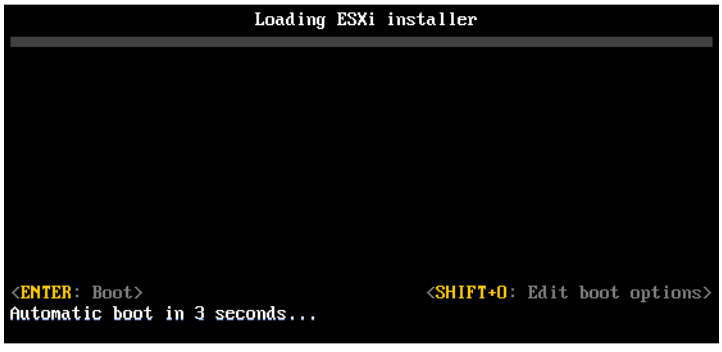
You can install or upgrade ESXi from a CD-ROM or DVD-ROM drive by using a script that specifies the installation or upgrade options.

Before you run the scripted installation or upgrade, verify that the following prerequisites are met:

- The system on which you are installing or upgrading meets the hardware requirements. See ESXi Hardware Requirements.
- You have the ESXi installer ISO on an installation CD or DVD . See Download and Burn the ESXi Installer ISO Image to a CD or DVD.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See About Installation and Upgrade Scripts.
- You have selected a boot command to run the scripted installation or upgrade. See Enter Boot Options to Run an Installation or Upgrade Script. For a complete list of boot commands, see Boot Options .

You can start the installation or upgrade script by entering a boot option when you start the host. You can also create an installer ISO image that includes the installation script. With an installer ISO image, you can perform a scripted, unattended installation when you boot the resulting installer ISO image. See Create an Installer ISO Image with a Custom Installation or Upgrade Script.

1. Boot the ESXi installer from the local CD-ROM or DVD-ROM drive.
2. When the ESXi installer window appears, press Shift+O to edit boot options.



3. Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

   The boot option has the form `ks=` .

4. Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Install or Upgrade ESXi from a USB Stick by Using a Script

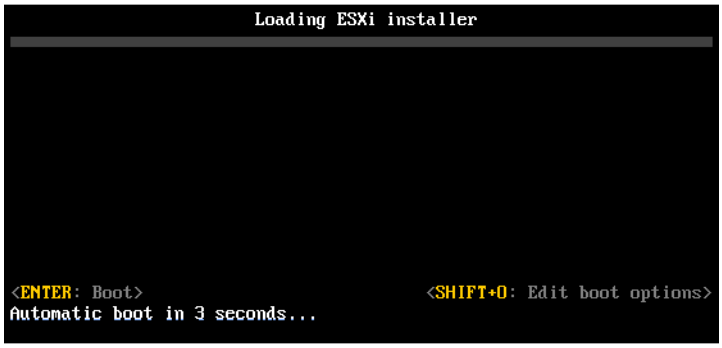
You can install or upgrade ESXi from a USB flash drive by using a script that specifies the installation or upgrade options.

Before running the scripted installation or upgrade, verify that the following prerequisites are met:

- The system that you are installing or upgrading to ESXi meets the hardware requirements for the installation or upgrade. See ESXi Hardware Requirements.
- You have the ESXi installer ISO on a bootable USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See About Installation and Upgrade Scripts.
- You have selected a boot option to run the scripted installation, upgrade, or migration. See Enter Boot Options to Run an Installation or Upgrade Script.

Supported boot options are listed in Boot Options .

1. Boot the ESXi installer from the USB flash drive.
2. When the ESXi installer window appears, press Shift+O to edit boot options.



3. Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

   The boot option has the form `ks=` .

4. Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Network Boot the ESXi Installer for a Scripted Installation or Upgrade

ESXi7.0 provides many options for booting the installer over a network and using an installation or upgrade script.

- For information about setting up a network infrastructure, see Network Booting the ESXi Installer.
- For information about creating and locating an installation script, see About Installation and Upgrade Scripts.
- For specific procedures to network boot the ESXi installer and use an installation script, see one of the following topics:
  - Boot the ESXi Installer by Using Native UEFI HTTP

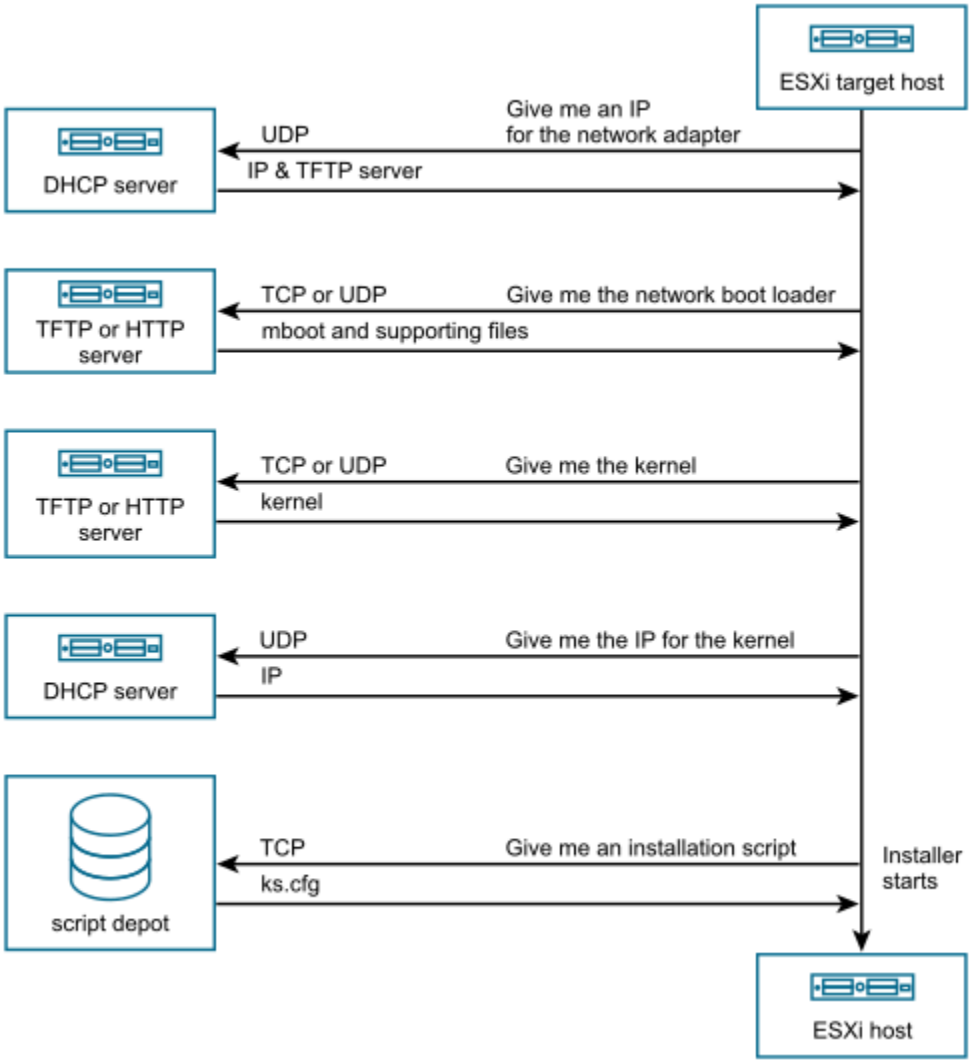
- Boot the ESXi Installer by Using iPXE and HTTP
- Boot the ESXi Installer by Using PXE and TFTP

Overview of the Network Boot Installation Process

You can boot an ESXi host from a network interface. The network boot process varies depending on whether the target host is using legacy BIOS or UEFI firmware, and whether the boot process uses PXE TFTP, iPXE HTTP, or UEFI HTTP.

When you boot a target host, it interacts with the different servers in the environment to get a network adapter, boot loader, kernel, IP address for the kernel, and finally an installation script. When all components are in place, installation starts, as shown in the following illustration.

Figure 5: Overview of PXE Boot Installation Process



The interaction between the ESXi host and other servers proceeds as follows:

1. The user boots the target ESXi host.
2. The target ESXi host makes a DHCP request.
3. The DHCP server responds with the IP information, the location of the TFTP or HTTP server, and the filename or URL of the initial network boot loader.

4. The ESXi host contacts the TFTP or HTTP server and requests the filename or URL that the DHCP server specified.
5. The TFTP or HTTP server sends the network boot loader, and the ESXi host runs it. The initial boot loader might load additional boot loader components from the server.
6. The boot loader searches for a configuration file on the TFTP or HTTP server, downloads the kernel and other ESXi components as specified in the configuration file, and boots the kernel on the ESXi host.
7. The installer runs interactively or using a kickstart script, as specified in the configuration file.

Boot the ESXi Installer by Using PXE and TFTP

You can use a TFTP server to PXE boot the ESXi installer. The process differs slightly depending on whether you use UEFI or boot from a legacy BIOS. Because most environments include ESXi hosts that support UEFI boot and hosts that support only legacy BIOS, this topic discusses prerequisites and steps for both types of hosts.

Verify that your environment meets the following prerequisites.

- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.
- Network adapter with PXE support on the target ESXi host.
- DHCP server that you can configure for PXE booting. See Sample DHCP Configurations.
- TFTP server.
- Network security policies to allow TFTP traffic (UDP port 69).
- For legacy BIOS, you can use only IPv4 networking. For UEFI PXE boot, you can use IPv4 or IPv6 networking.
- (Optional) Installation script (kickstart file).
- Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

For legacy BIOS systems, obtain version 3.86 of the SYSLINUX package. For more information, see Network Boot Background Information.

- For legacy BIOS machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `pxelinux.0` initial boot loader for all target machines, but potentially different PXELINUX configuration files depending on the target machine's MAC address.
- For UEFI machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

1. If your ESXi host runs legacy BIOS firmware only, obtain and configure PXELINUX.
   a) Obtain SYSLINUX version 3.86, unpack it, and copy the `pxelinux.0` file to the top-level `/tftpboot` directory on your TFTP server.
   b) Create a PXELINUX configuration file using the following code model.

      `ESXi-7.x.x-XXXXXX` is the name of the TFTP subdirectory that contains the ESXi installer files.

      ```
      DEFAULT install
      NOHALT 1
      LABEL install
        KERNEL ESXi-7.x.x-XXXXXX/mboot.c32
        APPEND -c ESXi-7.x.x-XXXXXX/boot.cfg
        IPAPPEND 2
      ```

c) Save the PXELINUX file in the `/tftpboot/pxelinux.cfg` directory on your TFTP server with a filename that will determine whether all hosts boot this installer by default:

Option	Description
Same installer	Name the file `default` if you want all host to boot this ESXi installer by default.
Different installers	Name the file with the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*) if you want only a specific host to boot with this file, for example, `01-23-45-67-89-0a-bc`.

2. If your ESXi host runs UEFI firmware, copy the `efi/boot/bootx64.efi` file from the ESXi installer ISO image to the `/tftpboot` folder on your TFTP server, and rename the file to `mboot.efi`. For 7.0 Update 3 and later, also copy the `efi/boot/crypto64.efi` file to the `/tftpboot` folder.

   Note: Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

3. Configure the DHCP server.
4. Create a subdirectory of your TFTP server's top-level `/tftpboot` directory and name it after the version of ESXi it will hold, for example, `/tftpboot/ESXi-7.x.x-xxxxx`.
5. Copy the contents of the ESXi installer image to the newly created directory.
6. Modify the `boot.cfg` file
   a) Add the following line:

      ```
      prefix=ESXi-7.x.x-xxxxxx
      ```

      Here, `ESXi-7.x.x-xxxxxx` is the pathname of the installer files relative to the TFTP server's root directory.
   b) If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.
   c) If the `kernelopt=` line contains the string `cdromBoot`, remove the string only.
7. Optional: For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option to the line after the kernel command, to specify the location of the installation script.

   Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory that contains the `ks.cfg` file.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

8. If your ESXi host runs UEFI firmware, specify whether you want all UEFI hosts to boot the same installer.

Option	Description
Same installer	Copy or link the `boot.cfg` file to `/tftpboot/boot.cfg`
Different installers	1. Create a subdirectory of `/tftpboot` named after the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), for example, `01-23-45-67-89-0a-bc`. 2. Place a copy of (or a link to) the host's `boot.cfg` file in that directory, for example, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`.

Boot the ESXi Installer by Using iPXE and HTTP

You can use iPXE to boot the ESXi installer from an HTTP server. The following topic discusses prerequisites and steps for ESXi hosts that support UEFI boot and hosts that support legacy BIOS only.

Verify that your environment has the following components:

- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.
- Network adapter with PXE support on the target ESXi host.
- DHCP server that you can configure for PXE booting. See Sample DHCP Configurations.
- TFTP server.
- Network security policies to allow TFTP traffic (UDP port 69).
- For legacy BIOS, you can use only IPv4 networking. For UEFI PXE boot, you can use IPv4 or IPv6 networking.
- (Optional) Installation script (kickstart file).
- Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Verify that your environment also meets the following prerequisites required for PXE boot using an HTTP Server:

- Verify that the HTTP server is accessible by your target ESXi hosts.
- If your ESXi host runs legacy BIOS firmware only, obtain version 3.86 of the SYSLINUX package. For more information, see Network Boot Background Information.
- For legacy BIOS machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `pxelinux.0` initial boot loader for all target machines, but potentially different PXELINUX configuration files depending on the target machine's MAC address.
- For UEFI machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

1. Obtain and configure iPXE.
   a) Obtain the iPXE source code.
   b) On the iPXE download page, follow the build instructions, but run one of the following commands.
      - For ESXi hosts that run legacy BIOS firmware only, run `make bin/undionly.kpxe`.
      - For ESXi hosts that run UEFI firmware, run `make bin-x86_64-efi/snponly.efi`.
   c) Copy the `undionly.kpxe` or `snponly.efi` file to the `/tftpboot` directory on your TFTP server.
2. If your ESXi host runs legacy BIOS firmware only, obtain and configure PXELINUX.
   a) Obtain SYSLINUX version 3.86, unpack it, and copy the `pxelinux.0` file to the `/tftpboot` directory on your TFTP server.
   b) Create a PXELINUX configuration file using the following code model.
      `ESXi-7.x.x-XXXXXX` is the name of the TFTP subdirectory that contains the ESXi installer files.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-7.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-7.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c) Save the PXELINUX file in the `/tftpboot/pxelinux.cfg` directory on your TFTP server.
      The filename determines whether all hosts boot this installer by default.

Option	Description
Same installer	Name the file `default` if you want all host to boot this ESXi installer by default.

Option	Description
Different installers	Name the file with the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), if only a specific host must boot this file. For example, `01-23-45-67-89-0a-bc`.

3. If your ESXi host runs UEFI firmware, copy the `efi/boot/bootx64.efi` file from the ESXi installer ISO image to the `/tftpboot` folder on your TFTP server, and rename the file to `mboot.efi`.

   Note: Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

4. Configure the DHCP server.
5. Create a directory on your HTTP server with the same name as the version of ESXi it will hold. For example, `/var/www/html/ESXi-7.x.x-XXXXXX`.
6. Copy the contents of the ESXi installer image to the newly created directory.
7. Modify the `boot.cfg` file
   a) Add the following line:

      ```
      prefix=http://XXX.XXX.XXX.XXX/ESXi-7.x.x-XXXXXX
      ```

      where `http://XXX.XXX.XXX.XXX/ESXi-7.x.x-XXXXXX` is the location of the installer files on the HTTP server.
   b) If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.
   c) If the `kernelopt=` line contains the string `cdromBoot`, remove the string only.
8. Optional: For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option to the line after the kernel command, to specify the location of the installation script.

   Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory that contains the `ks.cfg` file.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

9. If your ESXi host runs UEFI firmware, specify whether you want all UEFI hosts to boot the same installer.

Option	Description
Same installer	Copy or link the `boot.cfg` file to `/tftpboot/boot.cfg`
Different installers	1. Create a subdirectory of `/tftpboot` named after the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), for example, `01-23-45-67-89-0a-bc`. 2. Place a copy of (or a link to) the host's `boot.cfg` file in that directory, for example, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`.

Boot the ESXi Installer by Using Native UEFI HTTP

You can boot the ESXi installer directly from an HTTP server, without additional software to support the process.

Verify that your environment has the following components:

- ESXi host with UEFI firmware that supports the HTTP boot feature.
- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.

- Network adapter with UEFI networking support on the target ESXi host.
- DHCP server that you can configure for UEFI HTTP booting. See Sample DHCP Configurations
- (Optional) Installation script (kickstart file).
- Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

UEFI HTTP supports booting multiple versions of the ESXi installer. You use the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

Note: Do not mix IPv4 or IPv6 networking during the boot process. Use either IPv4 or IPv6 networking.

1. Copy the `efi/boot/bootx64.efi` file from the ESXi installer ISO image to a directory on your HTTP server and rename the file to `mboot.efi`. For example, `http://www.example.com/esxi/mboot.efi`.

   Note: Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

2. Configure the DHCP server.
3. Create a directory on your HTTP server with the same name as the version of ESXi it will hold. For example, `http://www.example.com/esxi/ESXi-7.x.x-XXXXXX`.
4. Copy the contents of the ESXi installer image to the newly created directory.
5. Modify the `boot.cfg` file.
   a) Add the following line with the URL of the newly created directory.

      ```
      prefix=http://www.example.com/esxi/ESXi-7.x.x-XXXXXX
      ```

   b) If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.
   c) If the `kernelopt=` line contains the string `cdromBoot`, remove the string only.
6. Optional: For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option to the line after the kernel command, to specify the location of the installation script.

   For example, `kernelopt=ks=http://www.example.com/esxi_ksFiles/ks.cfg`
7. Optional: Starting with ESXi 7.0 Update 2, you can use the virtual machine configuration parameters *`networkBootProtocol`* and *`networkBootUri`* to specify from where a virtual machines can boot. The setting *`networkBootProtocol`* specifies the boot protocol, IPv4 or IPv6. For example, `networkBootProtocol = httpv4` . The setting *`networkBootUri`* specifies the HTTP URL to the ESXi bootloader (bootx64.efi). For example, `networkBootUri = http://192.168.30.6/esxi70uc1/efi/boot/bootx64.efi` .
8. Specify whether you want all UEFI hosts to boot the same installer.

Option	Description
Same installer	Add the `boot.cfg` file to the same directory as `mboot.efi`. For example, `http://www.example.com/esxi/boot.cfg`
Different installers	1. Create a subdirectory of the directory that contains the `mboot.efi` file. Name the directory as the MAC address of the target host machine (01-*`mac_address_of_target_ESXi_host`*), for example, `01-23-45-67-89-0a-bc`. 2. Add the custom `boot.cfg` file in the directory. For example, `http://www.example.com/esxi/01-23-45-67-89-0a-bc/boot.cfg`.

   You can use both installer types. ESXi hosts without custom `boot.cfg` file on your HTTP server, boot from the default `boot.cfg` file.

Network Boot Background Information

Understanding the network boot process can help you during troubleshooting.

TFTP Server

Trivial File Transfer Protocol (TFTP) is similar to the FTP service, and is typically used only for network booting systems or loading firmware on network devices such as routers. TFTP is available on Linux and Windows.

- Most Linux distributions include a copy of the tftp-hpa server. If you require a supported solution, purchase a supported TFTP server from your vendor of choice. You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.
- If your TFTP server runs on a Microsoft Windows host, use tftpd32 version 2.11 or later. See http://tftpd32.jounin.net/.

SYSLINUX and PXELINUX

If you are using PXE in a legacy BIOS environment, you must understand the different boot environments.

- SYSLINUX is an open-source boot environment for machines that run legacy BIOS firmware. The ESXi boot loader for BIOS systems, `mboot.c32`, runs as a SYSLINUX plugin. You can configure SYSLINUX to boot from several types of media, including disk, ISO image, and network. You can find the SYSLINUX package at http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX is a SYSXLINUX configuration for booting from a TFTP server according to the PXE standard. If you use PXELINUX to boot the ESXi installer, the `pxelinux.0` binary file, `mboot.c32`, the configuration file, the kernel, and other files are transferred by TFTP.

Note: VMware builds the `mboot.c32` plugin to work with SYSLINUX version 3.86 and tests PXE booting only with that version. Other versions might be incompatible. *The Open Source Disclosure Package for VMware vSphere Hypervisor* includes bug fixes for SYSLINUX version 3.86.

iPXE

iPXE is open-source software that provides an implementation of HTTP. You can use the software to perform an initial boot. For more information, see https://ipxe.org/.

VMware includes a build of iPXE as part of Auto Deploy. The source tree for this build is available in *The Open Source Disclosure Package for VMware vCenter Server*.

UEFI PXE and UEFI HTTP

Most UEFI firmware natively includes PXE support that allows booting from a TFTP server. The firmware can directly load the ESXi boot loader for UEFI systems, `mboot.efi`. Additional software such as PXELINUX is not required.

Some UEFI firmware support native UEFI HTTP boot. The feature is introduced in version 2.5 of the UEFI specification. The firmware can load the ESXi boot loader from an HTTP server, without additional software, such as iPXE.

Note: Apple Macintosh products do not include PXE boot support. They include support for network booting through an Apple-specific protocol instead.

Alternative Approaches to Network Booting

Alternative approaches to network booting different software on different hosts are also possible, for example:

- Configuring the DHCP server to provide different initial boot loader filenames to different hosts depending on MAC address or other criteria. See your DCHP server's documentation.
- Approaches using iPXE as the initial bootloader with an iPXE configuration file that selects the next bootloader based on the MAC address or other criteria.

PXELINUX Configuration Files

You need a PXELINUX configuration file to boot the ESXi installer on a legacy BIOS system. The configuration file defines the menu displayed to the target ESXi host as it starts.

This section gives general information about PXELINUX configuration files.

For syntax details, see the SYSLINUX website at http://www.syslinux.org/.

Required Files

In the PXE configuration file, you must include paths to the following files:

- `mboot.c32` is the boot loader.
- `boot.cfg` is the boot loader configuration file.

See About the boot.cfg File

Filename for the PXE Configuration File

For the filename of the PXE configuration file, select one of the following options:

- `01-`*`mac_address_of_target_ESXi_host`*. For example, `01-23-45-67-89-0a-bc`
- The target ESXi host IP address in a hexadecimal notation.
- `default`

The initial boot file `pxelinux.0` tries to load a PXE configuration file in the following order:

1. It tries with the MAC address of the target ESXi host, prefixed with its ARP type code, which is 01 for Ethernet.
2. If that attempt fails, it tries with the hexadecimal notation of target ESXi system IP address.
3. Ultimately, it tries to load a file named `default`.

File Location for the PXE Configuration File

Save the file in `/tftpboot/pxelinux.cfg/` on the TFTP server.

For example, you might save the file on the TFTP server at `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. The MAC address of the network adapter on the target ESXi host is 00-21-5a-ce-40-f6.

Sample DHCP Configurations

The DHCP server must send the address of the TFTP or HTTP server and the filename of the initial boot loader to the ESXi host.

When the target machine first boots, it broadcasts a packet across the network requesting information to boot itself. The DHCP server responds. The DHCP server must be able to determine whether the target machine is allowed to boot and the location of the initial boot loader binary. For PXE boot, the location is a file on a TFTP server. For UEFI HTTP boot, the location is a URL.

CAUTION: Do not set up a second DHCP server if your network already has one. If multiple DHCP servers respond to DHCP requests, machines can obtain incorrect or conflicting IP addresses, or can fail to receive the proper boot information. Talk to a network administrator before setting up a DHCP server. For support on configuring DHCP, contact your DHCP server vendor.

There are many DHCP servers that you can use. The following examples are for an ISC DHCP server. If you are using a version of DHCP for Microsoft Windows, see the DHCP server documentation to determine how to pass the next-server and filename arguments to the target machine.

Example of Booting Using PXE and TFTP with IPv4

This example shows how to configure an ISC DHCP server to PXE boot ESXi using a TFTP server at IPv4 address xxx.xxx.xxx.xxx.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      filename = "mboot.efi";
   } else {
      filename = "pxelinux.0";
   }
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `pxelinux.0` or `mboot.efi` binary file on the TFTP server.

Example of Booting Using PXE and TFTP with IPv6

This example shows how to configure an ISC DHCPv6 server to PXE boot ESXi using a TFTP server at IPv6 address xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `mboot.efi` binary file on the TFTP server.

Example of Booting Using iPXE and HTTP with IPv4

This example shows how to configure an ISC DHCP server to boot ESXi by loading iPXE from a TFTP server at IPv4 address `xxx.xxx.xxx.xxx`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
```

```
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load mboot.efi as secondary bootloader
         filename = "mboot.efi";
      } else {
         # Load the snponly.efi configuration of iPXE as initial bootloader
         filename = "snponly.efi";
      }
   } else {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load pxelinux as secondary bootloader
         filename = "pxelinux.0";
      } else {
         # Load the undionly configuration of iPXE as initial bootloader
         filename = "undionly.kpxe";
   }
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `undionly.kpxe` or `snponly.efi` binary file on the TFTP server. In the legacy BIOS case, iPXE then asks the DHCP server for the next file to load, and the server returns `pxelinux.0` as the filename. In the UEFI case, iPXE then asks the DHCP server for the next file to load, and this time the server returns `mboot.efi` as the filename. In both cases, iPXE is resident and the system has HTTP capability. As a result, the system can load additional files from an HTTP server.

Example of Booting Using iPXE and HTTP with IPv6

This example shows how to configure an ISC DHCPv6 server to boot ESXi by loading iPXE from a TFTP server at IPv6 address `xxxx:xxxx:xxxx:xxxx::xxxx`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
   # Instruct iPXE to load mboot.efi as secondary bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
   # Load the snponly.efi configuration of iPXE as initial bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `snponly.efi` (iPXE) binary file on the TFTP server. iPXE then asks the DHCP server for the next file to load, and this time the server returns `mboot.efi` as the filename. iPXE is resident and the system has HTTP capability. As a result, the system can load additional files from an HTTP server.

Example of Booting Using UEFI HTTP with IPv4

This example shows how to configure an ISC DHCP server to boot ESXi by using native UEFI HTTP over IPv4 from Web server `www.example.com`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "httpclients" {
   match if substring(option vendor-class-identifier, 0, 10) = "HTTPClient";
   option vendor-class-identifier "HTTPClient";

   if option client-system-arch = 00:10 {
      # x86_64 UEFI HTTP client
      filename = http://www.example.com/esxi/mboot.efi;
   }
}
```

Example of Booting Using UEFI HTTP with IPv6

This example shows how to configure an ISC DHCPv6 server to boot ESXi by using native UEFI HTTP over IPv6 from Web server `www.example.com`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
option dhcp6.user-class code 15 = { integer 16, string };
option dhcp6.vendor-class code 16 = { integer 32, integer 16, string };

if option dhcp6.client-arch-type = 00:10 {
      # x86_64 HTTP clients
      option dhcp6.vendor-class 0 10 "HTTPClient";
      option dhcp6.bootfile-url "http://www.example.com/esxi/mboot.efi";
}
```

Installing ESXi Using vSphere Auto Deploy

vSphere Auto Deploy lets you provision hundreds of physical hosts with ESXi software.

Using Auto Deploy, experienced system administrators can manage large deployments efficiently. Hosts are network-booted from a central Auto Deploy server. Optionally, hosts are configured with a host profile of a reference host. The host profile can be set up to prompt the user for input. After boot up and configuration complete, the hosts are managed by vCenter Server just like other ESXi hosts.

Auto Deploy can also be used for stateless caching or stateful installs.

Important: Auto Deploy requires a secure separation between the production network and the management or deployment networks as discussed in vSphere Auto Deploy Security Considerations. Using Auto Deploy without this separation is insecure.

Stateless caching	By default, Auto Deploy does not store ESXi configuration or state on the host disk. Instead, an image profile defines the image that the host is provisioned with, and other host attributes are managed through host profiles. A host that uses Auto Deploy for stateless caching still needs to connect to the Auto Deploy server and the vCenter Server.
Stateful installs	You can provision a host with Auto Deploy and set up the host to store the image to disk. On subsequent boots, the host boots from disk.

Understanding vSphere Auto Deploy

vSphere Auto Deploy can provision hundreds of physical hosts with ESXi software.

You can specify the image to deploy and the hosts to provision with the image. Optionally, you can specify host profiles to apply to the hosts, a vCenter Server location (datacenter, folder or cluster), and assign a script bundle for each host.

Introduction to vSphere Auto Deploy

When you start a physical host that is set up for vSphere Auto Deploy, vSphere Auto Deploy uses PXE boot infrastructure in conjunction with vSphere host profiles to provision and customize that host. No state is stored on the host itself. Instead, the vSphere Auto Deploy server manages state information for each host.

State Information for ESXi Hosts

vSphere Auto Deploy stores the information for the ESXi hosts to be provisioned in different locations. Information about the location of image profiles and host profiles is initially specified in the rules that map machines to image profiles and host profiles.

Table 16: vSphere Auto Deploy Stores Information for Deployment

Information Type	Description	Source of Information
Image state	The executable software to run on an ESXi host.	Image profile, created with vSphere ESXi Image Builder.
Configuration state	The configurable settings that determine how the host is configured, for example, virtual switches and their settings, driver settings, boot parameters, and so on.	Host profile, created by using the host profile UI. Often comes from a template host.
Dynamic state	The runtime state that is generated by the running software, for example, generated private keys or runtime databases.	Host memory, lost during reboot.
Virtual machine state	The virtual machines stored on a host and virtual machine autostart information (subsequent boots only).	Virtual machine information sent by vCenter Server to vSphere Auto Deploy must be available to supply virtual machine information to vSphere Auto Deploy.
User input	State that is based on user input, for example, an IP address that the user provides when the system starts up, cannot automatically be included in the host profile.	Host customization information, stored by vCenter Server during first boot. You can create a host profile that requires user input for certain values.

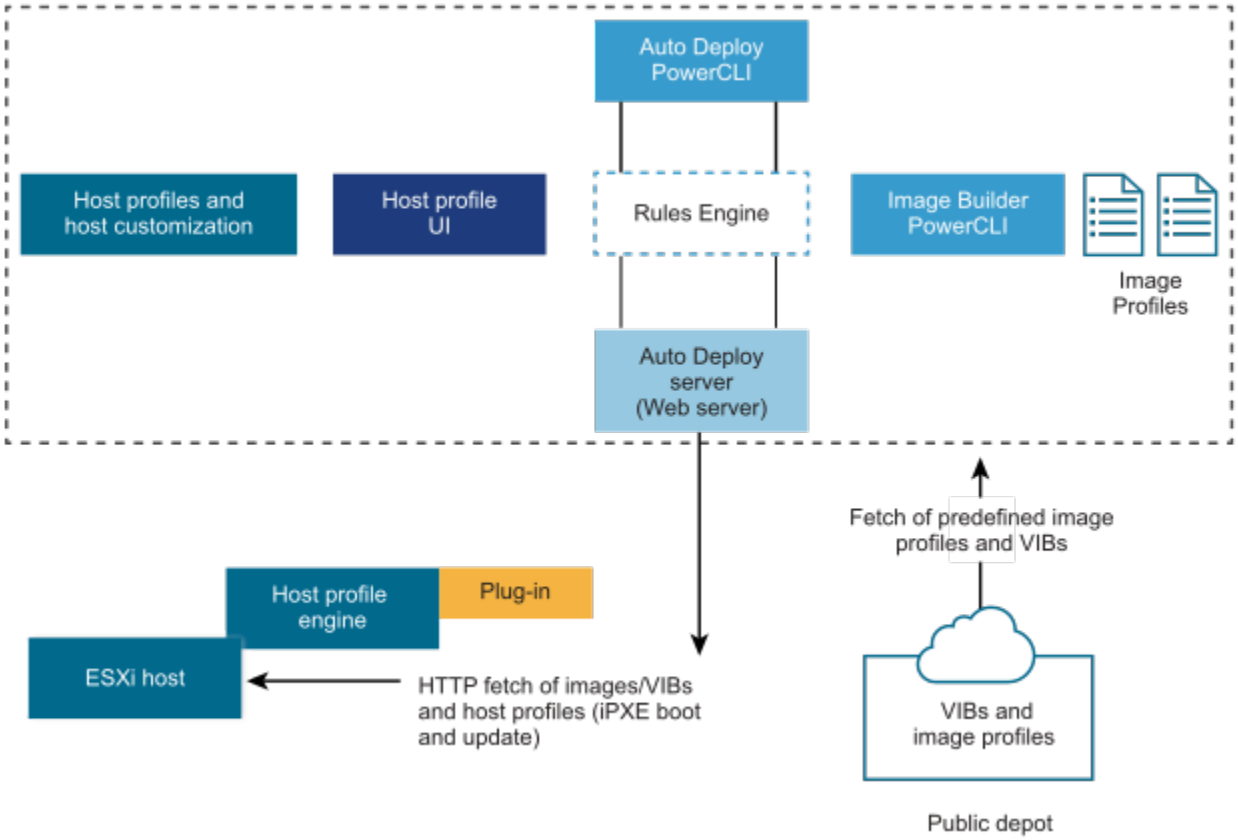
Information Type	Description	Source of Information
		When vSphere Auto Deploy applies a host profile that requires user provided information, the host is placed in maintenance mode. Use the host profile UI to check the host profile compliance, and respond to the prompt to customize the host.

vSphere Auto Deploy Architecture

The vSphere Auto Deploy infrastructure consists of several components.

For more information, watch the video "Auto Deploy Architecture":

Figure 6: vSphere Auto Deploy Architecture



vSphere Auto Deploy server

Serves images and host profiles to ESXi hosts.

vSphere Auto Deploy rules engine

Image profiles

Define the set of VIBs to boot ESXi hosts with.

- VMware and VMware partners make image profiles and VIBs available in public depots. Use vSphere ESXi Image Builder to examine the depot and use the vSphere Auto Deploy rules engine to specify which image profile to assign to which host.

Host profiles

Host customization

Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host.

For more information about host customizations, see the *vSphere Host Profiles* documentation.

Host customization was called answer file in earlier releases of vSphere Auto Deploy.

Rules and Rule Sets

You specify the behavior of the vSphere Auto Deploy server by using a set of rules. The vSphere Auto Deploy rules engine checks the rule set for matching host patterns to decide which items (image profile, host profile, vCenter Server location, or script object) to provision each host with.

The rules engine maps software and configuration settings to hosts based on the attributes of the host. For example, you can deploy image profiles or host profiles to two clusters of hosts by writing two rules, each matching on the network address of one cluster.

For hosts that have not yet been added to a vCenter Server system, the vSphere Auto Deploy server checks with the rules engine before serving image profiles, host profiles, and inventory location information to hosts. For hosts that are managed by a vCenter Server system, the image profile, host profile, and inventory location that vCenter Server has stored in the host object is used. If you make changes to rules, you can use the vSphere Client or vSphere Auto Deploy cmdlets in a PowerCLI session to test and repair rule compliance. When you repair rule compliance for a host, that host's image profile and host profile assignments are updated.

The rules engine includes rules and rule sets.

Rules

Rules can assign image profiles and host profiles to a set of hosts, or specify the location (folder or cluster) of a host on the target vCenter Server system. A rule can identify target hosts by boot MAC address, SMBIOS information, BIOS UUID, Vendor, Model, or fixed DHCP IP address. In most cases, rules apply to multiple hosts. You create rules by using the vSphere Client or vSphere Auto Deploy cmdlets in a PowerCLI session. After you create a rule, you must add it to a rule set. Only two rule sets, the active rule set and the working rule set, are supported. A rule can belong to both sets, the default, or only to the working rule set. After you add a rule to a rule set, you can no longer change the rule. Instead, you copy the rule and replace items or patterns in the copy. If you are managing vSphere Auto Deploy with the vSphere Client, you can edit a rule if it is in inactive state.

You can specify the following parameters in a rule.

Parameter	Description
Name	Name of the rule, specified with the `-Name` parameter.
Item	One or more items, specified with the `-Item` parameter. An item can be an image profile, a host profile, a vCenter Server inventory location (datacenter, folder, cluster) for the target host, or a custom script. You can specify multiple items separated by commas.
Pattern	The pattern specifies the host or group of hosts to which the rule applies.

Parameter	Description	
	vendor	Machine vendor name.
	model	Machine model name.
	serial	Machine serial number.
	hostname	Machine hostname.
	domain	Domain name.
	ipv4	IPv4 address of the machine.
	ipv6	IPv6 address of the machine. PXE booting with BIOS firmware is possible only with IPv4, PXE booting with UEFI firmware is possible with either IPv4 or IPv6.
	mac	Boot NIC MAC address.
	asset	Machine asset tag.
	oemstring	OEM-specific strings in the SMBIOS.
	You can specify `-AllHosts` to apply the item or items to all hosts.	

Active Rule Set

When a newly started host contacts the vSphere Auto Deploy server with a request for an image profile, the vSphere Auto Deploy server checks the active rule set for matching rules. The image profile, host profile, vCenter Server inventory location, and script object that are mapped by matching rules are then used to boot the host. If more than one item of the same type is mapped by the rules, the vSphere Auto Deploy server uses the item that is first in the rule set.

Working Rule Set

The working rule set allows you to test changes to rules before making the changes active. For example, you can use vSphere Auto Deploy cmdlets for testing compliance with the working rule set. The test verifies that hosts managed by a vCenter Server system are following the rules in the working rule set. By default, cmdlets add the rule to the working rule set and activate the rules. Use the `NoActivate` parameter to add a rule only to the working rule set.

You use the following workflow with rules and rule sets.

1. Make changes to the working rule set.
2. Test the working rule set rules against a host to make sure that everything is working correctly.
3. Refine and retest the rules in the working rule set.
4. Activate the rules in the working rule set.
   If you add a rule in a PowerCLI session and do not specify the `NoActivate` parameter, all rules that are currently in the working rule set are activated. You cannot activate individual rules.

See the PowerCLI command-line help and Managing vSphere Auto Deploy with PowerCLI Cmdlets for more information on using vSphere Auto Deploy with PowerCLI cmdlets. See Managing vSphere Auto Deploy with the vSphere Client for more information on using vSphere Auto Deploy with the vSphere Client.

vSphere Auto Deploy Boot Process

When you boot a host that you want to provision or reprovision with vSphere Auto Deploy, the vSphere Auto Deploy infrastructure supplies the image profile and, optionally, a host profile, a vCenter Server location, and script bundle for that host.

The boot process is different for hosts that have not yet been provisioned with vSphere Auto Deploy (first boot) and for hosts that have been provisioned with vSphere Auto Deploy and added to a vCenter Server system (subsequent boot).

First Boot Prerequisites

Before a first boot process, you must set up your system. Setup includes the following tasks, which are discussed in more detail in Preparing for vSphere Auto Deploy.

- Set up a DHCP server that assigns an IP address to each host upon startup and that points the host to the TFTP server to download the iPXE boot loader from.
- If the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, verify that the vSphere Auto Deploy server has an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.
- Identify an image profile to be used in one of the following ways.
  - Choose an ESXi image profile in a public depot.
  - Create a custom image profile by using vSphere ESXi Image Builder, and place the image profile in a depot that the vSphere Auto Deploy server can access. The image profile must include a base ESXi VIB.
- If you have a reference host in your environment, export the host profile of the reference host and define a rule that applies the host profile to one or more hosts. See Setting Up a vSphere Auto Deploy Reference Host.
- Specify rules for the deployment of the host and add the rules to the active rule set.

First Boot Overview

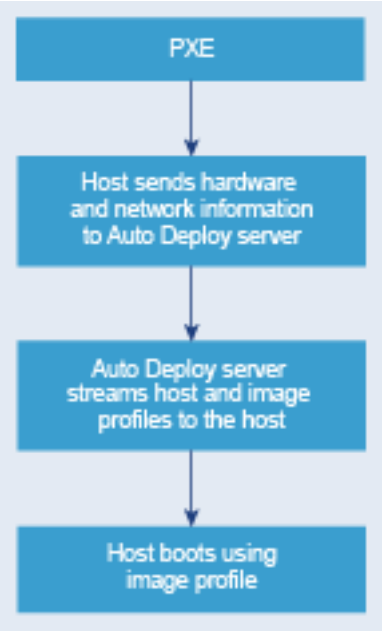
When a host that has not yet been provisioned with vSphere Auto Deploy boots (first boot), the host interacts with several vSphere Auto Deploy components.

1. When the administrator turns on a host, the host starts a PXE boot sequence.
   The DHCP Server assigns an IP address to the host and instructs the host to contact the TFTP server.
2. The host contacts the TFTP server and downloads the iPXE file (executable boot loader) and an iPXE configuration file.
3. iPXE starts executing.
   The configuration file instructs the host to make a HTTP boot request to the vSphere Auto Deploy server. The HTTP request includes hardware and network information.

4. In response, the vSphere Auto Deploy server performs these tasks:
   a. Queries the rules engine for information about the host.
   b. Streams the components specified in the image profile, the optional host profile, and optional vCenter Server location information.
5. The host boots using the image profile.
   If the vSphere Auto Deploy server provided a host profile, the host profile is applied to the host.
6. vSphere Auto Deploy adds the host to the vCenter Server system that vSphere Auto Deploy is registered with.
   a. If a rule specifies a target folder or cluster on the vCenter Server system, the host is placed in that folder or cluster. The target folder must be under a data center.
   b. If no rule exists that specifies a vCenter Server inventory location, vSphere Auto Deploy adds the host to the first datacenter displayed in the vSphere Client UI.
7. If the host profile requires the user to specify certain information, such as a static IP address, the host is placed in maintenance mode when the host is added to the vCenter Server system.
   You must reapply the host profile and update the host customization to have the host exit maintenance mode. When you update the host customization, answer any questions when prompted.
8. If the host is part of a DRS cluster, virtual machines from other hosts might be migrated to the host after the host has successfully been added to the vCenter Server system.

See Provision a Host (First Boot).

Figure 7: vSphere Auto Deploy Installation, First Boot



Subsequent Boots Without Updates

For hosts that are provisioned with vSphere Auto Deploy and managed by a vCenter Server system, subsequent boots can become completely automatic.

1. The administrator reboots the host.
2. As the host boots up, vSphere Auto Deploy provisions the host with its image profile and host profile.

3. Virtual machines are brought up or migrated to the host based on the settings of the host.
   - Standalone host. Virtual machines are powered on according to autostart rules defined on the host.
   - DRS cluster host. Virtual machines that were successfully migrated to other hosts stay there. Virtual machines for which no host had enough resources are registered to the rebooted host.

If the vCenter Server system is unavailable, the host contacts the vSphere Auto Deploy server and is provisioned with an image profile. The host continues to contact the vSphere Auto Deploy server until vSphere Auto Deploy reconnects to the vCenter Server system.

vSphere Auto Deploy cannot set up vSphere distributed switches if vCenter Server is unavailable, and virtual machines are assigned to hosts only if they participate in an HA cluster. Until the host is reconnected to vCenter Server and the host profile is applied, the switch cannot be created. Because the host is in maintenance mode, virtual machines cannot start. See Reprovision Hosts with Simple Reboot Operations.

Any hosts that are set up to require user input are placed in maintenance mode. See Update the Host Customization in the vSphere Client.

Subsequent Boots With Updates

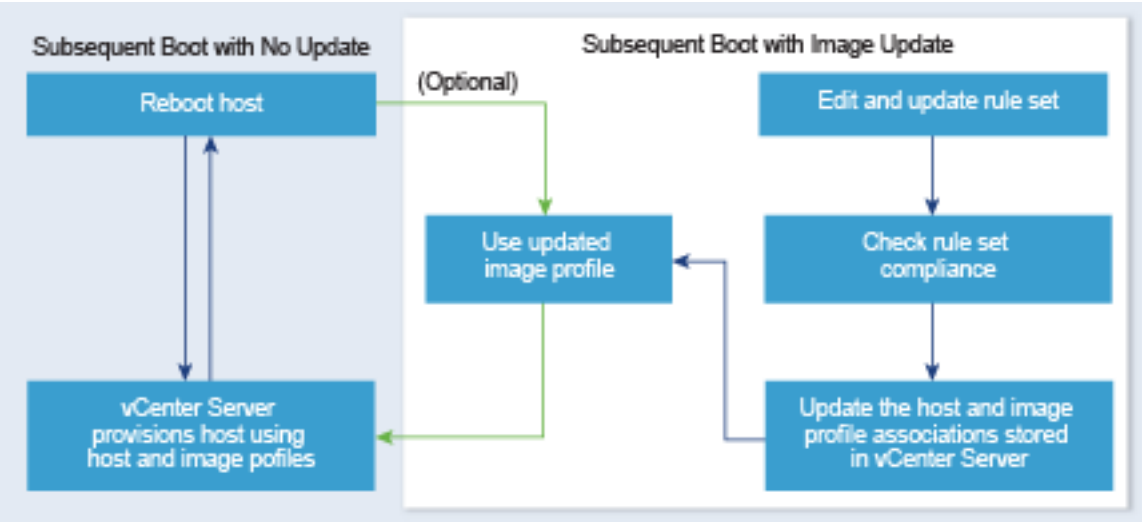
You can change the image profile, host profile, vCenter Server location, or script bundle for hosts. The process includes changing rules and testing and repairing the host's rule compliance.

1. The administrator uses the `Copy-DeployRule`PowerCLI cmdlet to copy and edit one or more rules and updates the rule set. See Overview of the vSphere Auto Deploy Process by Using PowerCLI for an example.
2. The administrator runs the `Test-DeployRulesetCompliance` cmdlet to check whether each host is using the information that the current rule set specifies.
3. The host returns a PowerCLI object that encapsulates compliance information.
4. The administrator runs the `Repair-DeployRulesetCompliance` cmdlet to update the image profile, host profile, or vCenter Server location the vCenter Server system stores for each host.
5. When the host reboots, it uses the updated image profile, host profile, vCenter Server location, or script bundle for the host.

   If the host profile is set up to request user input, the host is placed in maintenance mode. Follow the steps in Update the Host Customization in the vSphere Client.

See Test and Repair Rule Compliance .

Figure 8: vSphere Auto Deploy Installation, Subsequent Boots



Provisioning of Systems that Have Distributed Switches

You can configure the host profile of a vSphere Auto Deploy reference host with a distributed switch.

When you configure the distributed switch, the boot configuration parameters policy is automatically set to match the network parameters required for host connectivity after a reboot.

When vSphere Auto Deploy provisions the ESXi host with the host profile, the host goes through a two-step process.

1. The host creates a standard virtual switch with the properties specified in the boot configuration parameters field.
2. The host creates the VMkernel NICs. The VMkernel NICs allow the host to connect to vSphere Auto Deploy and to the vCenter Server system.

When the host is added to vCenter Server, vCenter Server removes the standard switch and reapplies the distributed switch to the host.

Note: Do not change the boot configuration parameters to avoid problems with your distributed switch.

Overview of the vSphere Auto Deploy Process by Using the vSphere Client

Getting started with vSphere Auto Deploy requires that you learn how vSphere Auto Deploy works, start the vSphere Auto Deploy and vSphere ESXi Image Builder vCenter Server services, create deploy rules that provision hosts, and power on your hosts to be booted with the image profile you specify.

The workflow for provisioning the hosts in your environment with vSphere Auto Deploy includes the following tasks:

1. Deploy vCenter Server.
   The vSphere Auto Deploy server is included.
2. Configure the vSphere Auto Deploy and vSphere ESXi Image Builder service startup types.
   See Prepare Your System for vSphere Auto Deploy and Configure the vSphere ESXi Image Builder.
3. Add or import a software depot to the vSphere Auto Deploy inventory.
   See Add a Software Depot or Import a Software Depot.
4. (Optional) If you want to create a custom image profile, clone, or create an image profile by using the vSphere Client.
   See Clone an Image Profile or Create an Image Profile.
5. Create a deploy rule that assigns the image profile to one host, to multiple hosts specified by a pattern, or to all hosts.
   See Create a Deploy Rule.
   Note: vSphere Auto Deploy is optimized for provisioning hosts that have a fixed MAC address to IP address mapping in DHCP (sometimes called DHCP reservations). If you want to use static IP addresses, you must set up the host profile to prompt for host customization. For more information, see the *vSphere Host Profiles* documentation.
6. Power on the hosts that you want to provision.
7. Set up the host you provisioned as a reference host for your host profile.
   You can specify the reference host syslog settings, firewall settings, storage, networking, and so on.
8. Extract a host profile from the reference host.
   See the *Host Profiles* documentation.
9. To provision multiple hosts with the host profile, clone or edit the previously created rule by using the vSphere Client.
   See Clone a Deploy Rule or Edit a Deploy Rule.
10. Activate the new rule and deactivate the old one.
    See Activate, Deactivate, and Reorder Deploy Rules.
11. Remediate the host associations to apply the new rule to the host.
    See Remediate a Non-compliant Host.

12. Verify that the hosts you provisioned meet the following requirements.
    - Each host is connected to the vCenter Server system.
    - The hosts are not in maintenance mode.
    - The hosts have no compliance failures.
    - Each host with a host profile that requires user input has up-to-date host customization information.

    Remediate host associations and compliance problems and reboot hosts until all hosts meet the requirements.

Read for an introduction to the boot process, differences between first and subsequent boots, and an overview of using host customization.

Overview of the vSphere Auto Deploy Process by Using PowerCLI

Getting started with vSphere Auto Deploy requires that you learn how vSphere Auto Deploy works, install the vSphere Auto Deploy server, install PowerCLI, write PowerCLI rules that provision hosts, and power on your hosts to be booted with the image profile you specify. You can customize of the image profile, host profile, and vCenter Server location.

See Set Up vSphere Auto Deploy and Provision Hosts with vSphere PowerCLI for a step-by-step exercise that helps you set up your first vSphere Auto Deploy environment.

To provision the hosts in your environment with vSphere Auto Deploy successfully, you can follow these steps.

1. Deploy vCenter Server.

   The vSphere Auto Deploy server is included.
2. Configure the vSphere Auto Deploy service startup type.

   See Prepare Your System for vSphere Auto Deploy.
3. Install PowerCLI, which includes vSphere Auto Deploy and vSphere ESXi Image Builder cmdlets.

   See Install vSphere ESXi Image Builder and Prerequisite Software, Using vSphere Auto Deploy Cmdlets, and Using VMware.Image Builder Cmdlets .
4. Find the image profile that includes the VIBs that you want to deploy to your hosts.
   - Usually, you add the depots containing the required software to your PowerCLI session, and then select an image profile from one of those depots.
   - To create a custom image profile, use vSphere ESXi Image Builder cmdlets to clone an existing image profile and add the custom VIBs to the clone. Add the custom image profile to the PowerCLI session.

   You must use vSphere ESXi Image Builder for customization only if you have to add or remove VIBs. In most cases, you can add the depot where VMware hosts the image profiles to your PowerCLI session as a URL.
5. Start a PowerCLI session and connect to the vCenter Server system that vSphere Auto Deploy is registered with.
6. Use the `New-DeployRule`PowerCLI cmdlet to write a rule that assigns the image profile to one host, to multiple hosts specified by a pattern, or to all hosts.

   ```
   New-DeployRule -Name "testrule" -Item image-profile -AllHosts
   ```

   See Assign an Image Profile to Hosts.

   Note: vSphere Auto Deploy is optimized for provisioning hosts that have a fixed MAC address to IP address mapping in DHCP (sometimes called DHCP reservations). If you want to use static IP addresses, you must set up the host profile to prompt for host customization. For more information, see the *vSphere Host Profiles* documentation.
7. Power on the hosts that you want to provision.
8. Set up the host you provisioned as a reference host for your host profile.

   You can specify the reference host syslog settings, firewall settings, storage, networking, and so on.
9. Set up the host you provisioned as a reference host for your host profile.

   You can specify the reference host syslog settings, firewall settings, storage, networking, and so on. See Setting Up a vSphere Auto Deploy Reference Host.
10. Create and export a host profile for the reference host.

    See the *Host Profiles* documentation.

11. To provision multiple hosts with the host profile, use the `Copy-DeployRule` cmdlet to edit the previously created rule. You can revise the rule to assign not only an image profile but also a host profile, a vCenter Server location, and a custom script bundle.

    ```
    Copy-DeployRule -DeployRule "testrule" -ReplaceItem my_host_profile_from_reference_host,my_target_cluster
                    -ReplacePattern  "ipv4=192.XXX.1.10-192.XXX.1.20"
    ```

    Where *my_host_profile_from_reference_host* is the name of the reference host profile, and *my_target_cluster* is the name of the target cluster.
12. Perform the test and repair compliance operations to remediate the hosts.
    See Test and Repair Rule Compliance .
13. Verify that the hosts you provisioned meet the following requirements.
    – Each host is connected to the vCenter Server system.
    – The hosts are not in maintenance mode.
    – The hosts have no compliance failures.
    – Each host with a host profile that requires user input has up-to-date host customization information.

    Remediate host associations and compliance problems and reboot hosts until all hosts meet the requirements.

Read for an introduction to the boot process, differences between first and subsequent boots, and an overview of using host customization.

Preparing for vSphere Auto Deploy

Before you can start using vSphere Auto Deploy, you must prepare your environment. You start with server setup and hardware preparation. You must configure the vSphere Auto Deploy service startup type in the vCenter Server system that you plan to use for managing the hosts you provision, and install PowerCLI.

Prepare Your System for vSphere Auto Deploy
Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.

- Verify that the hosts that you plan to provision with vSphere Auto Deploy meet the hardware requirements for ESXi. See ESXi Hardware Requirements.
- Verify that the ESXi hosts have network connectivity to vCenter Server and that all port requirements are met. See *vCenter Server Upgrade*.
- Verify that you have a TFTP server and a DHCP server in your environment to send files and assign network addresses to the ESXi hosts that Auto Deploy provisions. See Install the TFTP Server and Prepare the DHCP Server for vSphere Auto Deploy Provisioning.
- Verify that the ESXi hosts have network connectivity to DHCP, TFTP, and vSphere Auto Deploy servers.
- If you want to use VLANs in your vSphere Auto Deploy environment, you must set up the end to end networking properly. When the host is PXE booting, the firmware driver must be set up to tag the frames with proper VLAN IDs. You must do this set up manually by making the correct changes in the UEFI/BIOS interface. You must also correctly configure the ESXi port groups with the correct VLAN IDs. Ask your network administrator how VLAN IDs are used in your environment.
- Verify that you have enough storage for the vSphere Auto Deploy repository. The vSphere Auto Deploy server uses the repository to store data it needs, including the rules and rule sets you create and the VIBs and image profiles that you specify in your rules.
  Best practice is to allocate 2 GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 400 MB. Determine how much space to reserve for the vSphere Auto Deploy repository by considering how many image profiles you expect to use.
- Obtain administrative privileges to the DHCP server that manages the network segment you want to boot from. You can use a DHCP server already in your environment, or install a DHCP server. For your vSphere Auto Deploy setup,

replace the `gpxelinux.0` filename with `snponly64.efi.vmw-hardwired` for UEFI or `undionly.kpxe.vmw-hardwired` for BIOS. For more information on DHCP configurations, see Sample DHCP Configurations.

- Secure your network as for any other PXE-based deployment method. vSphere Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or the vSphere Auto Deploy server is not checked during a PXE boot.
- If you want to manage vSphere Auto Deploy with PowerCLI cmdlets, verify that Microsoft .NET Framework 4.5 or 4.5.x and Windows PowerShell 3.0 or 4.0 are installed on a Windows machine. See the *vSphere PowerCLI User's Guide*.
- Set up a remote Syslog server. See the *vCenter Server and Host Management* documentation for Syslog server configuration information. Configure the first host you boot to use the remote Syslog server and apply that host's host profile to all other target hosts. Optionally, install and use VMware vCenter Log Insight, which provides log aggregation and analytics for VMware and non-VMware products, virtual and physical, with near real-time search and analytics of log events.
- If the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, verify that the vSphere Auto Deploy server has an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

If you want to manage vSphere Auto Deploy with PowerCLI cmdlets, see *Set Up vSphere Auto Deploy and Provision Hosts with vSphere PowerCLI*.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Auto Deploy** page, select your vCenter Server from the drop-down menu at the top.
3. Click **Enable Auto Deploy and Image Builder** to activate the service.

   If the **Image Builder** service is already active, select the **Configure** tab and click **Enable Auto Deploy Service**.

   The **Software Depot** page appears.
4. Configure the TFTP server.
   a) Click the **Configure** tab.
   b) Click **Download TFTP Boot Zip** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.
   c) Optional: To use a proxy server, click **Add** on the *Auto Deploy Runtime Summary* pane and enter a proxy server URL in the text box.

      Using reverse proxy servers can offload the requests made to the vSphere Auto Deploy server.
5. Set up your DHCP server to point to the TFTP server on which the TFTP ZIP file is located.
   a) Specify the TFTP Server's IP address in DHCP option 66, frequently called next-server.
   b) Specify the boot filename, which is `snponly64.efi.vmw-hardwired` for UEFI or `undionly.kpxe.vmw-hardwired` for BIOS in the DHCP option 67, frequently called `boot-filename`.
6. Set each host you want to provision with vSphere Auto Deploy to network boot or PXE boot, following the manufacturer's instructions.
7. Optional: If you set up your environment to use Thumbprint mode, you can use your own Certificate Authority (CA) by replacing the OpenSSL certificate `rbd-ca.crt` and the OpenSSL private key `rbd-ca.key` with your own certificate and key file.

   The files are in `/etc/vmware-rbd/ssl/`.

   By default, vCenter Server uses VMware Certificate Authority (VMCA).

When you start an ESXi host that is set up for vSphere Auto Deploy, the host contacts the DHCP server and is directed to the vSphere Auto Deploy server, which provisions the host with the image profile specified in the active rule set.

- You can change the default configuration properties of the **Auto Deploy Service**. For more information, see "Configuring vCenter Server" in the *vCenter Server and Host Management* documentation.
- You can change the default configuration properties of the **Image Builder Service**. For more information, see "Configuring vCenter Server" in the *vCenter Server and Host Management* documentation.
- Configure the first host that you provision as a reference host. Use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for the reference host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- If you have to configure host-specific information, set up the host profile of the reference host to prompt for user input. For more information about host customizations, see the *vSphere Host Profiles* documentation.

Related Links

Using vSphere Auto Deploy Cmdlets on page 1069
vSphere Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. Users of vSphere Auto Deploy cmdlets can take advantage of all PowerCLI features.

Set Up Bulk Licensing on page 1070
You can use the vSphere Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with vSphere Auto Deploy.

Using vSphere Auto Deploy Cmdlets

vSphere Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. Users of vSphere Auto Deploy cmdlets can take advantage of all PowerCLI features.

Experienced PowerShell users can use vSphere Auto Deploy cmdlets just like other PowerShell cmdlets. If you are new to PowerShell and PowerCLI, the following tips might be helpful.

You can type cmdlets, parameters, and parameter values in the PowerCLI shell.

- Get help for any cmdlet by running `Get-Help`*`cmdlet_name`* .
- Remember that PowerShell is not case sensitive.
- Use tab completion for cmdlet names and parameter names.
- Format any variable and cmdlet output by using `Format-List` or `Format-Table`, or their short forms `fl` or `ft`. For more information, run the `Get-Help Format-List` cmdlet.

Passing Parameters by Name

You can pass in parameters by name in most cases and surround parameter values that contain spaces or special characters with double quotes.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

Most examples in the *vCenter Server Installation and Setup* documentation pass in parameters by name.

Passing Parameters as Objects

You can pass parameters as objects if you want to perform scripting and automation. Passing in parameters as objects is useful with cmdlets that return multiple objects and with cmdlets that return a single object. Consider the following example.

1. Bind the object that encapsulates rule set compliance information for a host to a variable.
   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```
2. View the `itemlist` property of the object to see the difference between what is in the rule set and what the host is currently using.
   ```
   $tr.itemlist
   ```

3. Remediate the host to use the revised rule set by using the `Repair-DeployRuleSetCompliance` cmdlet with the variable.

```
Repair-DeployRuleSetCompliance $tr
```

The example remediates the host the next time you boot the host.

Related Links

Prepare Your System for vSphere Auto Deploy on page 1067
Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.

Set Up Bulk Licensing on page 1070
You can use the vSphere Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with vSphere Auto Deploy.

Set Up Bulk Licensing

You can use the vSphere Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with vSphere Auto Deploy.

#unique_200.

Assigning license keys through the vSphere Client and assigning licensing by using PowerCLI cmdlets function differently.

Assign license keys with the vSphere Client	You can assign license keys to a host when you add the host to the vCenter Server system or when the host is managed by a vCenter Server system.
Assign license keys with LicenseDataManager PowerCLI	You can specify a set of license keys to be added to a set of hosts. The license keys are added to the vCenter Server database. Each time a host is added to the vCenter Server system or reconnects to it, the host is assigned a license key. A license key that is assigned through PowerCLI is treated as a default license key. When an unlicensed host is added or reconnected, it is assigned the default license key. If a host is already licensed, it keeps its license key.

The following example assigns licenses to all hosts in a data center. You can also associate licenses with hosts and clusters.

The following example is for advanced PowerCLI users who know how to use PowerShell variables.

1. In a PowerCLI session, connect to the vCenter Server system you want to use and bind the associated license manager to a variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

2. Run a cmdlet that retrieves the data center in which the hosts for which you want to use the bulk licensing feature are located.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

   You can also run a cmdlet that retrieves a cluster to use bulk licensing for all hosts in a cluster, or retrieves a folder to use bulk licensing for all hosts in a folder.

3. Create a `LicenseData` object and a `LicenseKeyEntry` object with associated type ID and license key.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
```

```
$licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere"
$licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

4. Associate the `LicenseKeys` attribute of the `LicenseData` object you created in step 3 with the `LicenseKeyEntry` object.

   ```
   $licenseData.LicenseKeys += $licenseKeyEntry
   ```

5. Update the license data for the data center with the `LicenseData` object and verify that the license is associated with the host container.

   ```
   $licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData)
   $licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
   ```

6. Provision one or more hosts with vSphere Auto Deploy and assign them to the data center or to the cluster that you assigned the license data to.
7. You can use the vSphere Client to verify that the host is successfully assigned to the default license `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` .

All hosts that you assigned to the data center are now licensed automatically.

Related Links

Prepare Your System for vSphere Auto Deploy on page 1067
Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.

Using vSphere Auto Deploy Cmdlets on page 1069
vSphere Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. Users of vSphere Auto Deploy cmdlets can take advantage of all PowerCLI features.

Managing vSphere Auto Deploy with PowerCLI Cmdlets

You can manage vSphere Auto Deploy with PowerCLI cmdlets to create rules that associate hosts with image profiles, host profiles, custom scripts and locations on the vCenter Server target. You can also update hosts by testing rule compliance and repairing compliance issues.

vSphere Auto Deploy PowerCLI Cmdlet Overview

You specify the rules that assign image profiles and host profiles to hosts using a set of PowerCLI cmdlets that are included in PowerCLI.

If you are new to PowerCLI, read the PowerCLI documentation and review Using vSphere Auto Deploy Cmdlets. You can get help for any command at the PowerShell prompt.

- Basic help: `Get-Help`*`cmdlet_name`*
- Detailed help: `Get-Help` *`cmdlet_name`*`-Detailed`

Note: When you run vSphere Auto Deploy cmdlets, provide all parameters on the command line when you invoke the cmdlet. Supplying parameters in interactive mode is not recommended.

Table 17: Rule Engine PowerCLI Cmdlets

Command	Description
`Get-DeployCommand`	Returns a list of vSphere Auto Deploy cmdlets.
`New-DeployRule`	Creates a new rule with the specified items and patterns.

Command	Description
`Set-DeployRule`	Updates an existing rule with the specified items and patterns. You cannot update a rule that is part of a rule set.
`Get-DeployRule`	Retrieves the rules with the specified names.
`Copy-DeployRule`	Clones and updates an existing rule.
`Add-DeployRule`	Adds one or more rules to the working rule set and, by default, also to the active rule set. Use the `NoActivate` parameter to add a rule only to the working rule set.
`Remove-DeployRule`	Removes one or more rules from the working rule set and from the active rule set. Run this command with the `-Delete` parameter to completely delete the rule.
`Set-DeployRuleset`	Explicitly sets the list of rules in the working rule set.
`Get-DeployRuleset`	Retrieves the current working rule set or the current active rule set.
`Switch-ActiveDeployRuleset`	Activates a rule set so that any new requests are evaluated through the rule set.
`Get-VMHostMatchingRules`	Retrieves rules matching a pattern. For example, you can retrieve all rules that apply to a host or hosts. Use this cmdlet primarily for debugging.
`Test-DeployRulesetCompliance`	Checks whether the items associated with a specified host are in compliance with the active rule set.
`Repair-DeployRulesetCompliance`	Given the output of `Test-DeployRulesetCompliance`, this cmdlet updates the image profile, host profile, and location for each host in the vCenter Server inventory. The cmdlet might apply image profiles, apply host profiles, or move hosts to prespecified folders or clusters on the vCenter Server system.
`Apply-EsxImageProfile`	Associates the specified image profile with the specified host.
`Get-VMHostImageProfile`	Retrieves the image profile in use by a specified host. This cmdlet differs from the `Get-EsxImageProfile` cmdlet in vSphere ESXi Image Builder.
`Repair-DeployImageCache`	Use this cmdlet only if the vSphere Auto Deploy image cache is accidentally deleted.
`Get-VMHostAttributes`	Retrieves the attributes for a host that are used when the vSphere Auto Deploy server evaluates the rules.
`Get-DeployMachineIdentity`	Returns a string value that vSphere Auto Deploy uses to logically link an ESXi host in vCenter Server to a physical machine.
`Set-DeployMachineIdentity`	Logically links a host object in the vCenter Server database to a physical machine. Use this cmdlet to add hosts without specifying rules.
`Get-DeployOption`	Retrieves the vSphere Auto Deploy global configuration options. This cmdlet currently supports the vlan-id option, which specifies the default VLAN ID for the ESXi Management Network of a host provisioned with vSphere Auto Deploy. vSphere Auto Deploy uses the value only if the host boots without a host profile.

Command	Description
`Set-DeployOption`	Sets the value of a global configuration option. Currently supports the vlan-id option for setting the default VLAN ID for the ESXi Management Network.
`Add-ProxyServer`	Adds a proxy server to the vSphere Auto Deploy database. Run the command with the `-Address` parameter to specify the IPv4 or IPv6 address. The address can include a port number.
`List-ProxyServer`	Lists the proxy servers that are currently registered with vSphere Auto Deploy.
`Delete-ProxyServer`	Deletes one or more proxy servers from the list of proxy servers that are registered with vSphere Auto Deploy. You can run the command with the `-id` parameter from the list of proxy servers or with the `-Address` parameter by specifying the IPv4 or IPv6 address of the proxy server you want to delete.
`Add-ScriptBundle`	Adds one or more script bundles to the vSphere Auto Deploy server.
`Get-ScriptBundle`	Retrieves the list of script bundles available on the vSphere Auto Deploy server and the scripts they contain.
`Remove-ScriptBundle`	Removes a script bundle from vSphere Auto Deploy. Applicable for vSphere version 6.7 and later.
`Get-CustomCertificate`	Retrieves the custom host certificate uploaded into AutoDeploy. You must run the command with the `-HostId [MAC_Address | BIOS_UUID]` parameter. The first time you add custom certificates, you don't see any certificates returned by this cmdlet.
`List-CustomCertificates`	Retrieves information about all custom host certificates used by Auto Deploy. The list provides details for the name of the certificate, `Host ID`, and `Associated Host Name`, which reflects the name of the vCenter Server for the Auto Deploy server.
`Add-CustomCertificate`	Adds a custom certificate to the VMware Endpoint Certificate Store and associates it with an ESXi host. The certificate becomes active upon host reboot. You can use the `Get-CustomCertificate` cmdlet to retrieve the custom host certificate key. You can run the command with the `-HostId [MAC_Address | BIOS_UUID]` parameter to associate the certificate to the host, specifying a `-Key [file:///path/to/key.key]` and `-Cert [file:///path/to/cert.crt]`. Using this cmdlet requires the **AutoDeploy.Rule.Create** privilege on the root folder of vCenter Server.
`Remove-CustomCertificate`	Removes a set of custom host certificates from Auto Deploy. The certificate entries are deleted from the database and the certificate files are removed from the filestore. Hosts that have already booted with a custom certificate must be rebooted to receive a new certificate. You must provide at least one of `-Cert` or `-HostId` parameters. Using this cmdlet requires the **AutoDeploy.Rule.Create** privilege on the root folder of vCenter Server.

Assign an Image Profile to Hosts

Before you can provision a host, you must create rules that assign an image profile to each host that you want to provision by using vSphere Auto Deploy.

vSphere Auto Deploy extensibility rules enforce that VIBs at the CommunitySupported level can only contain files from certain predefined locations, such as the ESXCLI plug-in path, jumpstart plug-in path, and so on. If you add a VIB that is in a different location to an image profile, a warning results. You can override the warning by using the `force` option.

If you call the `New-DeployRule` cmdlet on an image profile that includes VIBs at the CommunitySupported level which violate the rule, set `$DeployNoSignatureCheck = $true` before adding the image profile. With that setting, the system ignores signature validation and does not perform the extensibility rules check.

Note: Image profiles that include VIBs at the CommunitySupported level are not supported on production systems.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Determine the location of a public software depot, or define a custom image profile by using vSphere ESXi Image Builder.

3. Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run `Add-EsxSoftwareDepot` *depot_url*.
ZIP file	1. Download the ZIP file to a local file path. 2. Run `Add-EsxSoftwareDepot C:\`*file_path*`\`*my_offline_depot*`.zip`.

4. In the depot, find the image profile that you want to use by running the `Get-EsxImageProfile` cmdlet.

   By default, the ESXi depot includes one base image profile that includes VMware tools and has the string `standard` in its name, and one base image profile that does not include VMware tools.

5. Define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to the image profile.

   ```
   New-DeployRule -Name "testrule" -Item "My Profile25" -Pattern "ven-
   dor=Acme,Zven", "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   Double quotes are required if a name contains spaces, optional otherwise. Specify `-AllHosts` instead of a pattern to apply the item to all hosts.

   The cmdlet creates a rule named `testrule`. The rule assigns the image profile named My Profile25 to all hosts with a vendor of Acme or Zven that also have an IP address in the specified range.

6. Add the rule to the rule set.

   ```
   Add-DeployRule testrule
   ```

   By default, the rule is added to both the working rule set and the active rule set. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

When the host boots from iPXE, it reports attributes of the machine to the console. Use the same format of the attributes when writing deploy rules.

```
**************************************************************
* Booting through VMware AutoDeploy...
```

```
*
* Machine attributes:
* . asset=No Asset Tag
* . domain=vmware.com
* . hostname=myhost.mycompany.com
* . ipv4=XX.XX.XXX.XXX
* . mac=XX:Xa:Xb:Xc:Xx:XX
* . model=MyVendorModel
* . oemstring=Product ID: XXXXXX-XXX
* . serial=XX XX XX XX XX XX...
* . uuid=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
* . vendor=MyVendor
****************************************************************
```

- For hosts already provisioned with vSphere Auto Deploy, perform the compliance testing and repair operations to provision them with the new image profile. See Test and Repair Rule Compliance .
- Turn on unprovisioned hosts to provision them with the new image profile.

Write a Rule and Assign a Host Profile to Hosts

vSphere Auto Deploy can assign a host profile to one or more ESXi hosts.

The host profile might include information about storage configuration, network configuration, or other characteristics of the host. If you add a host to a cluster, that cluster's host profile is used.

- Install PowerCLI and all prerequisite software. For information, see vCenter Server Installation and Setup.
- Export the host profile that you want to use.

In many cases, you assign a host to a cluster instead of specifying a host profile explicitly. The host uses the host profile of the cluster.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Using the vSphere Client, set up a host with the settings you want to use and create a host profile from that host.
3. Find the name of the host profile by running `Get-VMhostProfile`PowerCLI cmdlet, passing in the ESXi host from which you create a host profile.
4. At the PowerCLI prompt, define a rule in which host profiles are assigned to hosts with certain attributes, for example a range of IP addresses.

   ```
   New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
    "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   The specified item is assigned to all hosts with the specified attributes. This example specifies a rule named testrule2. The rule assigns the specified host profile *`my_host_profile`* to all hosts with an IP address inside the specified range and with a manufacturer of Acme or Zven.

5. Add the rule to the rule set.

   ```
   Add-DeployRule testrule2
   ```

   By default, the working rule set becomes the active rule set, and any changes to the rule set become active when you add a rule. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

- Assign a host already provisioned with vSphere Auto Deploy to the new host profile by performing compliance test and repair operations on those hosts. For more information, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the host profile.

Write a Rule and Assign a Host to a Folder or Cluster

vSphere Auto Deploy can assign a host to a folder or cluster. When the host boots, vSphere Auto Deploy adds it to the specified location on the vCenter Server. Hosts assigned to a cluster inherit the cluster's host profile.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Verify that the folder you select is in a data center or in a cluster. You cannot assign the host to a standalone top-level folder.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to a folder or a cluster.

   ```
   New-DeployRule -Name testrule3 -Item "my folder" -Pattern "vendor=Acme,Zven",
    "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   This example passes in the folder by name. You can instead pass in a folder, cluster, or data center object that you retrieve with the `Get-Folder`, `Get-Cluster`, or `Get-Datacenter` cmdlet.

3. Add the rule to the rule set.

   ```
   Add-DeployRule testrule3
   ```

   By default, the working rule set becomes the active rule set, and any changes to the rule set become active when you add a rule. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

- Assign a host already provisioned with vSphere Auto Deploy to the new folder or cluster location by performing test and repair compliance operation. See Test and Repair Rule Compliance .
- Power on unprovisioned hosts to add them to the specified vCenter Server location.

Configure a Stateless System by Running a Custom Script

You can use vSphere Auto Deploy to configure one or more hosts by associating custom scripts with a vSphere Auto Deploy rule.

- Prepare your system for vSphere Auto Deploy. For more information, see *vSphere Installation and Setup*.
- Verify that the script bundle you want to associate with a vSphere Auto Deploy rule is in `.tgz` format, with a maximum size of 10 MB, and written in Python or BusyBox ash scripting language.

The scripts run in alphabetical order after the initial ESXi boot workflow of the host.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Run the `Add-ScriptBundle` cmdlet to add the script bundle that contains the necessary scripts to the vSphere Auto Deploy inventory.

   ```
   Add-ScriptBundle c:/temp/MyScriptBundle.tgz
   ```

   The name of the script bundle without the `.tgz` extension is the name identifier or object of the script bundle item. You can update an existing script bundle by using the `-Update` parameter with the `Add-ScriptBundle` cmdlet.

3. Optional: Run the `Get-ScriptBundle` cmdlet to verify that the script bundle is added to the vSphere Auto Deploy inventory.
4. Define a rule in which hosts with certain attributes, for example a range of IP addresses, are assigned to the script bundle.

   ```
   New-DeployRule -Name "testrule4" -Item "MyScriptBundle" -Pattern "ven-
   dor=Acme,Zven", "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   Double quotes are required if a name contains spaces, optional otherwise. Specify `-AllHosts` instead of a pattern to apply the item to all hosts.

   You create a rule named *testrule4*. The rule assigns the script bundle named My Script Bundle to all hosts with a vendor of Acme or Zven that also have an IP address in the specified range. You can use the name identifier of the script bundle or the object returned by the `Get-ScriptBundle` cmdlet to identify the script bundle you want to associate with the rule.
5. Add the rule to the rule set.

   ```
   Add-DeployRule testrule4
   ```

   By default, the rule is added to both the working rule set and the active rule set. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

- For hosts already provisioned with vSphere Auto Deploy, perform the compliance testing and repair operations to provision them with the new scripts. See Test and Repair Rule Compliance .
- Turn on unprovisioned hosts to provision them with the new scripts.

Test and Repair Rule Compliance

Test new or modified rules for compliance and repair accordingly, as changes in the vSphere Auto Deploy rule set are not updated automatically.

When you add a rule to the vSphere Auto Deploy rule set or modify one or more rules, hosts are not updated automatically. vSphere Auto Deploy applies the new rules only when you test their rule compliance and perform remediation.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Verify that your infrastructure includes one or more ESXi hosts provisioned with vSphere Auto Deploy, and that the host on which you installed PowerCLI can access those ESXi hosts.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.
2. Use PowerCLI to check which vSphere Auto Deploy rules are currently available.

   ```
   Get-DeployRule
   ```

   The system returns the rules and the associated items and patterns.
3. Modify one of the available rules.

   For example, you can change the image profile and the name of the rule.

   ```
   Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
   ```

   You cannot edit a rule already added to the active rule set. Instead, you can copy the rule and replace the item or pattern you want to change.

4. Verify that you can access the host for which you want to test rule set compliance.

   ```
   Get-VMHost -Name MyEsxi42
   ```

5. Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

6. Examine the differences between the contents of the rule set and configuration of the host.

   ```
   $tr.itemlist
   ```

   If the host for which you want to test the new rule set compliance is compliant with the active rule set, the system returns a table of current and expected items.

   ```
   CurrentItem                          ExpectedItem
   -----------                          ------------
   My Profile 25MyNewProfile
   ```

7. Remediate the host to use the revised rule set the next time you boot the host.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

If the rule you changed specified the inventory location, the change takes effect when you repair compliance. For all other changes, reboot your host to have vSphere Auto Deploy apply the new rule and to achieve compliance between the rule set and the host.

Register a Caching Proxy Server Address with vSphere Auto Deploy

Simultaneously booting large number of stateless hosts places a significant load on the vSphere Auto Deploy server. You can load balance the requests between the vSphere Auto Deploy server and one or more proxy servers that you register with vSphere Auto Deploy.

- Prepare your system for vSphere Auto Deploy. For more information, see *vSphere Installation and Setup*.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Register a caching proxy server addresses with vSphere Auto Deploy by running the `Add-ProxyServer` cmdlet.

   ```
   Add-ProxyServer -Address 'https://proxy_server_ip_address:port_number'
   ```

   You can run the cmdlet multiple times to register multiple proxy servers. The address can contain a port number.

3. Optional: Run the `List-ProxyServer` cmdlet to verify that the caching proxy server is registered with vSphere Auto Deploy.

Managing vSphere Auto Deploy with the vSphere Client

You can add ESXi hosts to the vSphere Auto Deploy inventory, create, monitor, and manage rules, and host associations by using the vSphere Client.

Create a Deploy Rule

Before you provision ESXi hosts with vSphere Auto Deploy, you must create rules that assign host locations, image profiles, and host profiles to the hosts. An ESXi host can match more than one vSphere Auto Deploy rule criteria, when this is the case, the rule order is considered.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- If you want to include an image profile to the rule, verify that the software depot you need is added to the inventory. See Add a Software Depotor Import a Software Depot.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, click **New Deploy Rule**.
   The **New Deploy Rule** wizard appears.
3. On the **Name and hosts** page of the wizard, enter a name for the new rule.
4. Select to either apply the rule to all hosts in the inventory or only to hosts that match a specific pattern.
   You can select one or more patterns.
   For example, the rule can apply only to hosts in a vCenter Single Sign-On domain, with a specific host name, or that match a specific IPv4 range.
5. On the **Configuration** page of the wizard, you can optionally include items in the rule.
   Each enabled item adds a new page to the wizard.

Option	Action
Host Location	Add the hosts that match the criteria of the rule to a specific location.
Image Profile	Assign an image profile to the hosts that match the rule criteria.
Host Profile	Assign a host profile to the hosts that match the rule criteria.
Script Bundle	Assign a script bundle to the host that match the rule criteria.

6. Optional: On the **Select host location** page of the wizard, select a data center, folder, or cluster as host location for the hosts that match the rule.
7. Optional: On the **Select image profile** page of the wizard, use the drop-down menu to select a software depot and choose an image profile from the list.
   If you want to bypass the acceptance level verification for the image profile, select the **Skip image profile signature check** check box.
8. Optional: On the **Select host profile** page of the wizard, select a host profile from the list.
9. Optional: On the **Select script bundle** page of the wizard, select a script bundle from the list.
10. On the **Ready to complete** page, review the summary information for the new rule.

You can view the newly created rule listed on the **Deploy Rules** tab.

- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.
- Edit a vSphere Auto Deploy rule. See Edit a Deploy Rule.
- Clone a vSphere Auto Deploy rule. See Clone a Deploy Rule.
- View the host location, image profile, host profile, and added script bundles. See View Host Associations.
- Remediate non-compliant hosts. See Remediate a Non-compliant Host.
- Change the image profile association of a host. See Edit the Image Profile Association of a Host.

Clone a Deploy Rule

You can use a vSphere Auto Deploy rule as a template and modify only parts of the rule instead of creating a new one.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Create a vSphere Auto Deploy rule. See Create a Deploy Rule.
- If you want to include an image profile to the rule, verify that the software depot you need is added to the inventory. See Add a Software Depotor Import a Software Depot.

You can clone an existing vSphere Auto Deploy rule by using the Clone Deploy Rule wizard.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, select a rule from the list.
3. Click **Clone**.
   The **Clone Deploy Rule** wizard appears.
4. On the **Name and hosts** page of the wizard, enter a name for the new rule.
5. Select to either apply the rule to all hosts in the inventory or only to hosts that match a specific pattern.
   You can select one or more patterns.
   For example, the rule can apply only to hosts in a vCenter Single Sign-On domain, with a specific host name, or that match a specific IPv4 range.
6. On the **Configuration** page of the wizard, you can optionally include items in the rule.
   Each enabled item adds a new page to the wizard.

Option	Action
Host Location	Add the hosts that match the criteria of the rule to a specific location.
Image Profile	Assign an image profile to the hosts that match the rule criteria.
Host Profile	Assign a host profile to the hosts that match the rule criteria.
Script Bundle	Assign a script bundle to the host that match the rule criteria.

7. On the **Select host location** page of the wizard, select a location for the hosts that match the rule.

Option	Action
If you want to keep the host location used in the cloned rule	Select the **Same Host location** check box.
If you want to select a new location for the selected hosts	1. Select the **Browse for Host location** check box. 2. Select a data center, folder, or cluster as host location. 3. Click **Next**.

8. On the **Select image profile** page of the wizard, select an image profile.

Option	Action
If you do not want to change the image profile	Select the **Same image profile** check box.
If you want to assign a new image profile to the selected hosts	1. Select the **Browse for Image Profile** check box. 2. Select a software depot from the drop-down menu. 3. Select an image profile from the list. 4. (Optional) If you want to bypass the acceptance level verification for the image profile, select the **Skip image profile signature check** check box.

9. On the **Select host profile** page of the wizard, select a host profile.

Option	Action
If you want to keep the host profile used in the cloned rule	Select the **Same Host profile** check box.
If you want to assign a new host profile to the selected hosts	1. Select the **Browse for Host Profile** check box. 2. Select a host profile from the list and click **Next**.

10. On the **Select script bundle** page of the wizard, select a script bundle from the list.
11. On the **Ready to complete** page, review the summary information for the new rule.

- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.
- Edit a vSphere Auto Deploy rule. See Edit a Deploy Rule.

Edit a Deploy Rule

You can edit the name of an Auto Deploy rule, its matching hosts, the host location, the image profile, and the host profile if the rule is inactive in the inventory.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Create a vSphere Auto Deploy rule. See Create a Deploy Rule.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, from the list of rules in the inventory select the rule and click **Edit**.

   The Edit Deploy Rule dialog box appears.
3. Optional: On the **Name and hosts** page of the wizard, enter a new name for the rule.
4. Select to either apply the rule to all hosts in the inventory or only to hosts that match a specific pattern.

   You can select one or more patterns.

   For example, the rule can apply only to hosts in a vCenter Single Sign-On domain, with a specific host name, or that match a specific IPv4 range.
5. On the **Configuration** page of the wizard, you can optionally include items in the rule.

   Each enabled item adds a new page to the wizard.

Option	Action
Host Location	Add the hosts that match the criteria of the rule to a specific location.
Image Profile	Assign an image profile to the hosts that match the rule criteria.
Host Profile	Assign a host profile to the hosts that match the rule criteria.
Script Bundle	Assign a script bundle to the host that match the rule criteria.

6. On the **Select host location** page of the wizard, select a location for the hosts that match the rule.

Option	Action
If you want to keep the host location used in the cloned rule	Select the **Same Host location** check box.
If you want to select a new location for the selected hosts	1. Select the **Browse for Host location** check box. 2. Select a data center, folder, or cluster as host location. 3. Click **Next**.

7. On the **Select image profile** page of the wizard, select an image profile.

Option	Action
If you do not want to change the image profile	Select the **Same image profile** check box.
If you want to assign a new image profile to the selected hosts	1. Select the **Browse for Image Profile** check box. 2. Select a software depot from the drop-down menu. 3. Select an image profile from the list. 4. (Optional) If you want to bypass the acceptance level verification for the image profile, select the **Skip image profile signature check** check box.

8. On the **Select host profile** page of the wizard, select a host profile.

Option	Action
If you want to keep the host profile used in the cloned rule	Select the **Same Host profile** check box.
If you want to assign a new host profile to the selected hosts	1. Select the **Browse for Host Profile** check box. 2. Select a host profile from the list and click **Next**.

9. On the **Select script bundle** page of the wizard, select a script bundle from the list.
10. On the **Ready to complete** page, review the summary information for the new rule.

- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.
- Clone a vSphere Auto Deploy rule. See Clone a Deploy Rule.

Activate, Deactivate, and Reorder Deploy Rules

After you create a vSphere Auto Deploy rule, the rule is in inactive state. You must activate the rule for it to take effect. You can use the Activate and Reorder wizard to activate, deactivate, and change the order of the rules.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Create a vSphere Auto Deploy rule. See Create a Deploy Rule.

The upper list on the **Activate and Reorder** page of the wizard displays the rules in the active rule set. The lower list displays the inactive rules.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, click **Activate/Deactivate rules**.

   The Activate and Reorder wizard appears.
3. Optional: If you want to deactivate an active rule, select the rule from the active rules list and click the **Deactivate** button.
4. From the list of inactive rules, select the rule that you want to activate and click the **Activate** button.
5. Optional: If you want to reorder the rules in the active rule list, select a rule that you want to move up or down in the list and click **Move up** or **Move down** above the list of active rules.

   The rules are listed by priority. For example, if two or more rules apply to the same host but are set to provision the host with different host locations, image profiles, and host profiles, the rule that is highest in the list takes effect on the host.

6. Optional: If you want to test an inactive rule before activation, click **Test rules before activation**.
   a) Select a host from the list and click **Check Compliance** to view the current status of the host and the changes that are expected after the activation of the rule.

      If the host is compliant with the rule, you do not need to remediate the host after you activate the rule.
   b) Optional: If you want to remediate the selected hosts after the rule activation, enable the toggle button or select the **Remediate all host associations after rule activation** check box to remediate all hosts.
7. Review the list of active rules and click **OK**.

On the **Deploy Rules** tab, the rule is listed as active in the Status column.

- View the host location, image profile, host profile, and added script bundles. See View Host Associations.
- Remediate non-compliant hosts. See Remediate a Non-compliant Host.

View Host Associations

Some of the hosts in the vSphere Auto Deploy inventory might not be compliant with the active deploy rules. To verify that one or more ESXi hosts are compliant with the active rule set, you must check the host associations compliance.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Create a vSphere Auto Deploy rule. See Create a Deploy Rule.
- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. Check the host associations compliance.

   The **Check Host Associations Compliance** window displays the status of the host and whether the host is compliant with the active rule set. You can view the currently assigned host location, image profile, host profile, script bundle, and the associations that will take effect after a remediation of the host.

Option	Steps
If you want to check the host associations compliance of a single host	1. On the **Deployed Hosts** tab, select an ESXi host. 2. Click **Check Host Associations Compliance**. 3. Check if the host associations are compliant with the current active rule set. 4. If you want to remediate the host, click **Remediate**. 5. Close the **Check Host Associations Compliance** window.
If you want to check the host associations compliance of multiple hosts	1. On the **Deployed Hosts** tab, select multiple ESXi hosts. 2. Click **Check Host Associations Compliance**. 3. Confirm that you want to check the compliance of all selected hosts. 4. Review the compliance status of the hosts in the left pane. 5. (Optional) Select a host to view the compliance status details. 6. (Optional) Select a host and click **Remediate** . 7. (Optional) Select the **Remediate all host associations after rule activation** check box to remediate all hosts. 8. **Close** the **Check Host Associations Compliance** window.

- Remediate non-compliant hosts. See Remediate a Non-compliant Host.
- Edit the image profile association of a host. See Edit the Image Profile Association of a Host.
- Edit a vSphere Auto Deploy rule. See Edit a Deploy Rule.

Edit the Image Profile Association of a Host

You can edit the image profile association of a single host if the host is not associated with a vSphere Auto Deploy rule or if you do not want to change the image profile association of multiple hosts by editing a rule.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Create a vSphere Auto Deploy rule. See Create a Deploy Rule.
- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deployed Hosts** tab, select an ESXi host.
3. Click **Edit Image Profile Association**.

   The Edit Image Profile Association dialog box appears.
4. Edit the image profile association of the host.

Option	Action
If you do not want to change the image profile	Select the **Same image profile** check box.
If you want to assign a new image profile to the selected hosts	1. Select the **Browse for Image Profile** check box. 2. Select a software depot from the drop-down menu. 3. Select an image profile from the list. 4. (Optional) If you want to bypass the acceptance level verification for the image profile, select the **Skip image profile signature check** check box.

5. Click **OK**.

The new image profile is listed in the Associated Image Profile column after a refresh of the page.

- View the host location, image profile, host profile, and added script bundles. See View Host Associations.
- If the host is associated with a rule and you want to revert to the image profile defined in the rule, remediate the host. See Remediate a Non-compliant Host.

Remediate a Non-compliant Host

When you add a rule to the vSphere Auto Deploy active rule set or make changes to one or more rules, hosts are not updated automatically. You must remediate the host associations to apply the new rules to the host.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Create a vSphere Auto Deploy rule. See Create a Deploy Rule.
- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.
- If the remediation of a host, results in a change in its location, the host must be placed in maintenance mode.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deployed Hosts** tab, select a single or multiple ESXi hosts.
3. Click **Remediate Host Associations**.

   If you remediate a host that has an edited image profile association, the host reverts to the settings defined in the rule that it matches.

   You can monitor the progress of the remediation process in the Recent Tasks pane.

- View the host location, image profile, host profile, and added script bundles. See View Host Associations.
- Change the image profile association of a host. See Edit the Image Profile Association of a Host.

Add a Host to the vSphere Auto Deploy Inventory

You can view the hosts that do not match any vSphere Auto Deploy rule and manually add a host to the vSphere Auto Deploy inventory.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- To assign an image profile to the host, add the software depot that you need to the inventory. See Add a Software Depot or Import a Software Depot.

To add a host to the current vSphere Auto Deploy inventory of deployed hosts, you can create a new rule or edit an existing rule to include a host that is not deployed with vSphere Auto Deploy and associate it with a specific host location, image profile, host profile, and script bundle. Alternatively, you can manually add a host to the inventory by assigning it a host location, image profile, host profile, and script bundle.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Discovered Hosts** tab, select one or more hosts that you want to provision with a host location, image profile, and host profile.
3. Select **Add to Inventory**.

   Alternatively, click **Remove** to dismiss the selected hosts from the **Discovered Hosts** tab.

   The Add to Inventory wizard appears.
4. On the **Select host location** page of the wizard, select a data center, folder, or cluster as host location for the hosts that match the rule.
5. On the **Select image profile** page of the wizard, use the drop-down menu to select a software depot and choose an image profile from the list.

   If you want to bypass the acceptance level verification for the image profile, select the **Skip image profile signature check** check box.
6. On the **Select host profile** page of the wizard, select a host profile from the list.
7. On the **Select host profile** page of the wizard, use the **Filter** to search the host profiles list or select the **Do not include a host profile** check box to continue without adding a host profile.
8. On the **Select script bundle** page of the wizard, select a script bundle from the list.
9. On the Ready to complete page, review the selected host associations.

- Edit a vSphere Auto Deploy rule. See Edit a Deploy Rule.
- Clone a vSphere Auto Deploy rule. See Clone a Deploy Rule.
- View the host location, image profile, host profile, and added script bundles. See View Host Associations.
- Remediate non-compliant hosts. See Remediate a Non-compliant Host.

Add a Host to a Cluster That Uses a Single Image

To add ESXi hosts to a cluster that you manage by an image, you create a rule in Auto Deploy that assigns a host location to the hosts.

- Prepare your system and install the Auto Deploy Server. For more information, see *Prepare Your System for vSphere Auto Deploy* in the *VMware ESXi Installation and Setup* documentation.
- Verify that each ESXi host is version 7.0 or later.

- Verify that all hosts in the cluster are stateful and have a physical storage attached.
- Verify that solutions, which are not integrated with vSphere Lifecycle Manager are not enabled for the cluster.

By creating an Auto Deploy rule, where the host target location is a cluster managed by an image, you can transition stateful ESXi hosts to the cluster. Based on host identification mechanisms, the rule adds the hosts to the target cluster.

Such Auto Deploy rule is not allowed to contain an Image Profile or a Host Profile, as the image specification and configuration of the target cluster define the same.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, click **New Deploy Rule**.
   The **New Deploy Rule** wizard appears.
3. On the **Name and hosts** page of the wizard, enter a name for the new rule.
4. Select to either apply the rule to all hosts in the inventory or only to hosts that match a specific pattern.
   You can select one or more patterns.
   For example, the rule can apply only to hosts in a vCenter Single Sign-On domain, with a specific host name, or that match a specific IPv4 range.
5. On the **Configuration** page of the wizard, select the **Host Location** check box, and click **Next**.
   You can optionally include a script bundle to the ESXi hosts that match the rule criteria by selecting the **Script Bundle** check box.

   Note: The image profile and host profile attached to the target cluster are used.
6. On the **Select host location** page of the wizard, select a cluster that uses a single image.
7. Optional: On the **Select script bundle** page of the wizard, select a script bundle from the list.
8. On the **Ready to complete** page, review the summary information for the new rule.
9. Click **Finish**.

You can view the newly created rule listed on the **Deploy Rules** tab.

- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.
- For more information on stateless caching and stateful installs, see Use vSphere Auto Deploy for Stateless Caching and Stateful Installs.

Working with Script Bundles

You can add a custom script for additional post-deployment host configuration. The script runs after you provision an ESXi host with Auto Deploy. For example, you can create a custom ESXi firewall rule and other configurations not available with Host Profiles.

- Verify that you can run the script in the ESXi Shell.

Since vSphere 6.7 Update 1, you can add or remove a custom script by using the vSphere Client. A script bundle can include multiple scripts and must be delivered as a single compressed file with the `.tgz` extension. After uploaded to the vCenter Server, you can include the script bundle to an Auto Deploy rule.

1. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.

2. Select the **Script Bundles** tab.
3. Click **Upload**.
4. Browse to a script bundle file and select **Upload**.
   The script is present in the **Script Bundles** list.
5. Optional: Select a script bundle, click **Remove**, and confirm the selection.
   The script bundle is deleted from the list.

- Activate a vSphere Auto Deploy rule. See Activate, Deactivate, and Reorder Deploy Rules.
- Edit a vSphere Auto Deploy rule. See Edit a Deploy Rule.
- Clone a vSphere Auto Deploy rule. See Clone a Deploy Rule.
- View the host location, image profile, host profile, and added script bundles. See View Host Associations.
- Remediate non-compliant hosts. See Remediate a Non-compliant Host.
- Change the image profile association of a host. See Edit the Image Profile Association of a Host.

Download vSphere Auto Deploy Logs

You can use the vSphere Auto Deploy logging information from the vSphere Client to resolve problems that you encounter with vSphere Auto Deploy.

Use the vSphere Client to log in to the vCenter Server instance that vSphere Auto Deploy is registered with.

1. Navigate to**Home** > **Administration** and select **Deployment** > **System Configuration**.
2. Select one of the nodes for which you want to retrieve a support bundle. The support bundle holds the services logs.
3. Click **Export Support Bundle**.
4. Select only **VirtualAppliance** > **Auto Deploy**.
5. Click the **Export Support Bundle** button to download the log files.

Start, Stop, or Restart the vSphere Auto Deploy Service

You can start, stop, or restart the Auto Deploy service in the vCenter Server Management Interface.

Verify that you have a root access to the vCenter Server Management Interface.

To start, stop, and restart services in vCenter Server, you use the vCenter Server Management Interface.

1. Log in to the vCenter Server Management Interface, https://*IP-address-or-FQDN*:5480.
2. Click **Services**.
   The **Services** pane displays a table of all installed services. You can sort them by name, startup type, health, and state.
3. Select the **Auto Deploy** service and select your action.
   The available actions depend on whether the Auto Deploy service is already running or not.
   - Click **Restart** to restart the service.

     Restarting the service requires confirmation and might lead to the Auto Deploy functionality becoming temporarily unavailable.
   - Click **Start** to start the service.
   - Click **Stop** to stop the service.

     Stopping the service requires confirmation.

Provisioning ESXi Systems with vSphere Auto Deploy

vSphere Auto Deploy can provision hundreds of physical hosts with ESXi software, either for first boot, reboot, or reprovisioning.

You can provision hosts that did not previously run ESXi software (first boot), reboot hosts, or reprovision hosts with a different image profile, host profile, custom script, or folder, or cluster location. The vSphere Auto Deploy process differs depending on the state of the host and on the changes that you want to make.

Provision a Host (First Boot)

Provisioning a host that has never been provisioned with vSphere Auto Deploy (first boot) differs from subsequent boot processes. You must prepare the host and fulfill all other prerequisites before you can provision the host. You can optionally define a custom image profile with vSphere ESXi Image Builder by using the vSphere Client or PowerCLI cmdlets.

- Make sure your host meets the hardware requirements for ESXi hosts.
- Prepare the system for vSphere Auto Deploy. See Preparing for vSphere Auto Deploy.
- Write rules that assign an image profile to the host and optionally assign a host profile and a vCenter Server location to the host. See Managing vSphere Auto Deploy with PowerCLI Cmdlets or Managing vSphere Auto Deploy with the vSphere Client.

  When the setup is complete, the vSphere Auto Deploy service is enabled, DHCP setup is complete, and rules for the host that you want to provision are in the active rule set.

1. Turn on the host.

   The host contacts the DHCP server and downloads iPXE from the location the server points it to. Next, the vSphere Auto Deploy server provisions the host with the image specified by the rule engine. The vSphere Auto Deploy server might also apply a host profile to the host if one is specified in the rule set. Finally, vSphere Auto Deploy adds the host to the vCenter Server system that is specified in the rule set.
2. Optional: If vSphere Auto Deploy applies a host profile that requires user input such as an IP address, the host is placed in maintenance mode. Reapply the host profile with the vSphere Client and provide the user input when prompted.

After the first boot process, the host is running and managed by a vCenter Server system. The vCenter Server stores the host's image profile, host profile, and location information.

You can now reboot the host as needed. Each time you reboot, the host is reprovisioned by the vCenter Server system.

Reprovision hosts as needed. See Reprovisioning Hosts.

If you want to change the image profile, host profile, custom script, or location of the host, update the rules and activate them by using the vSphere Client or perform a test and repair compliance operation in a PowerCLI session. See Rules and Rule Sets or Test and Repair Rule Compliance .

Reprovisioning Hosts

Use vSphere Auto Deploy to reprovision ESXi hosts with a different image profile or a different host profile.

vSphere Auto Deploy supports multiple reprovisioning options. You can perform a simple reboot or reprovision with a different image profile or a different host profile.

The following reprovisioning operations are available.

- Simple reboot.
- Reboot of hosts for which the user answered questions during the boot operation.
- Reprovision with a different image profile.
- Reprovision with a different host profile.

Reprovision Hosts with Simple Reboot Operations

You can reprovisions ESXi hosts with the image profile, host profile, custom script, and vCenter Server location assigned during first boot.

A simple reboot of a host that is provisioned with vSphere Auto Deploy requires only that all prerequisites are still met. The process uses the previously assigned image profile, host profile, custom script, and vCenter Server location.

- Verify that all associated items like are available. An item can be an image profile, host profile, custom script or vCenter Server inventory location.
- Verify that the host has the identifying information (asset tag, IP address) it had during previous boot operations.

1. Place the host in maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

2. Reboot the host.

The host shuts down. When the host reboots, it uses the image profile that the vSphere Auto Deploy server provides. The vSphere Auto Deploy server also applies the host profile stored on the vCenter Server system.

Reprovision a Host with a New Image Profile by Using PowerCLI

You can use vSphere Auto Deploy to reprovision a host with a new image profile in a PowerCLI session by changing the rule for the host and performing a test and repair compliance operation.

- Verify that the setup you performed during the first boot operation is in place.

Several options for reprovisioning hosts exist.

- If the VIBs that you want to use support live update, you can use an `esxcli software vib` command. In that case, you must also update the rule set to use an image profile that includes the new VIBs.
- During testing, you can apply an image profile to an individual host with the `Apply-EsxImageProfile` cmdlet and reboot the host so the change takes effect. The `Apply-EsxImageProfile` cmdlet updates the association between the host and the image profile but does not install VIBs on the host.
- In all other cases, use this procedure.

1. At the PowerShell prompt, run the `Connect-VIServer`PowerCLI cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Determine the location of a public software depot that contains the image profile that you want to use, or define a custom image profile with vSphere ESXi Image Builder.

3. Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run `Add-EsxSoftwareDepot depot_url`.
ZIP file	1. Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine. 2. Run `Add-EsxSoftwareDepot C:\file_path \my_offline_depot.zip`.

4. Run `Get-EsxImageProfile` to see a list of image profiles, and decide which profile you want to use.
5. Run `Copy-DeployRule` and specify the `ReplaceItem` parameter to change the rule that assigns an image profile to hosts.

   The following cmdlet replaces the current image profile that the rule assigns to the host with the *`my_new_imageprofile`* profile. After the cmdlet completes, `myrule` assigns the new image profile to hosts. The old version of `myrule` is renamed and hidden.

   ```
   Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
   ```

6. Test the rule compliance for each host that you want to deploy the image to.
   a) Verify that you can access the host for which you want to test rule set compliance.

      ```
      Get-VMHost -Name ESXi_hostname
      ```

   b) Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

      ```
      $tr = Test-DeployRuleSetCompliance ESXi_hostname
      ```

   c) Examine the differences between the contents of the rule set and configuration of the host.

      ```
      $tr.itemlist
      ```

      The system returns a table of current and expected items if the host for which you want to test the new rule set compliance is compliant with the active rule set.

      ```
      CurrentItem                          ExpectedItem
      -----------                          ------------
      my_old_imageprofilemy_new_imageprofile
      ```

   d) Remediate the host to use the revised rule set the next time you boot the host.

      ```
      Repair-DeployRuleSetCompliance $tr
      ```

7. Reboot the host to provision it with the new image profile.

Reprovision a Host with a New Image Profile by Using the vSphere Client

You can use vSphere Auto Deploy to reprovision a host with a new image profile with the vSphere Client by changing the rule that the host corresponds to and activating the rule.

- Verify that the image profile you want to use to reprovision the host is available. See Create an Image Profile.
- Verify that the setup you performed during the first boot operation is in place.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Deploy Rules** tab, from the list of rules in the inventory select the rule and click **Edit**.

   The Edit Deploy Rule dialog box appears.
3. Optional: On the **Name and hosts** page of the wizard, enter a name for the new rule.
4. Optional: Select to either apply the rule to all hosts in the inventory or only to hosts that match a specific pattern.

   You can select one or more patterns.

   For example, the rule can apply only to hosts in a vCenter Single Sign-On domain, with a specific host name, or that match a specific IPv4 range.

5. On the **Configuration** page of the wizard, you can optionally include items in the rule.
   Each enabled item adds a new page to the wizard.

Option	Action
Host Location	Add the hosts that match the criteria of the rule to a specific location.
Image Profile	Assign an image profile to the hosts that match the rule criteria.
Host Profile	Assign a host profile to the hosts that match the rule criteria.
Script Bundle	Assign a script bundle to the host that match the rule criteria.

6. Click **Next** to skip the Host Location selection.
7. On the **Select image profile** page of the wizard, assign an image profile to the hosts that match the rule criteria.

Option	Action
If you do not want to change the image profile	Select the **Same image profile** check box.
If you want to assign a new image profile to the selected hosts	1. Select the **Browse for Image Profile** check box. 2. Select a software depot from the drop-down menu. 3. Select an image profile from the list. 4. (Optional) If you want to bypass the acceptance level verification for the image profile, select the **Skip image profile signature check** check box.

8. Click **Next** to skip the Host profile selection.
9. On the **Ready to complete** page, review the summary information for the new image profile and click **Finish**.
10. Click **Activate/Deactivate rules**.
11. From the list of inactive rules, select the rule that you want to activate and click the **Activate** button.
12. Optional: If you want to reorder the rules in the active rule list, select a rule that you want to move up or down in the list and click **Move up** or **Move down** above the list of active rules.
    The rules are listed by priority. For example, if two or more rules apply to the same host but are set to provision the host with different host locations, image profiles, and host profiles, the rule that is highest in the list takes effect on the host.
13. Optional: If you want to test an inactive rule before activation, click **Test rules before activation**.
    a) Select a host from the list and click **Check Compliance** to view the current status of the host and the changes that are expected after the activation of the rule.
       If the host is compliant with the rule, you do not need to remediate the host after you activate the rule.
    b) Optional: If you want to remediate the selected hosts after the rule activation, enable the toggle button or select the **Remediate all host associations after rule activation** check box to remediate all hosts.
14. Review the list of active rules and click **OK**.
15. Reboot the host to provision it with the new image profile.

Update the Host Customization in the vSphere Client

If a host required user input during a previous boot, the answers are saved with the vCenter Server. If you want to prompt the user for new information, you must remediate the host.

Attach a host profile that prompts for user input to the host.

1. Migrate all virtual machines to different hosts, and place the host into maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

2. Navigate to **Home** > **Auto Deploy**.
   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
3. On the **Deployed Hosts** tab, select an ESXi host.
4. Click **Remediate Host Associations**.
   You can monitor the progress of the remediation process in the Recent Tasks pane.
5. When prompted, provide the user input.
6. Direct the host to exit maintenance mode.

The host customization is saved and takes effect the next time you boot the host.

Provision ESXi Host by Using an Image Profile Without VMware Tools
When you provision v hosts with vSphere Auto Deploy, you can select to provision the hosts with an image profile that does not contain VMware Tools binaries. This image profile is smaller, has a lower memory overhead, and boots faster in a PXE-boot environment.

Download the *xxxxx*-no-tools image profile from the VMware download site.

If the network boot time is too slow when using the standard image, or if you want to save space on the hosts, you can use an image profile that does not include VMware Tools and place the VMware Tools binaries on a shared storage.

1. Boot an ESXi host that was not provisioned with vSphere Auto Deploy.
2. Copy the /productLocker directory from the ESXi host to a shared storage.
   You can connect to an ESXi host using an SSH client, see Knowledge Base article1019852.
3. Change the *UserVars.ProductLockerLocation* variable to point to the new /productLocker directory location.
   a) In the vSphere Client, select the reference host and click the **Configure** tab.
   b) Under **System**, click **Advanced System Settings**.
   c) Click **Edit**.
   d) Filter the settings for uservars, and select **UserVars.ProductLockerLocation**.
   e) Click the current value and edit the location so it points to the shared storage.
4. Create a host profile from the reference host.
5. Create a vSphere Auto Deploy rule that assigns the *xxxxx*-no-tools image profile and host profile from the reference host to all other hosts.
6. Boot your target hosts with the rule so they pick up the product locker location from the reference host.

Use vSphere Auto Deploy for Stateless Caching and Stateful Installs

With stateless caching, you can cache the image of an ESXi host. With stateful installs, you can install hosts over the network.

The vSphere Auto Deploy stateless caching feature lets you cache the host's image. The vSphere Auto Deploy stateful installs feature lets you install hosts over the network. After the initial network boot, these hosts boot like other ESXi hosts. The stateless caching solution is primarily intended for situations when several hosts boot simultaneously. The locally cached image helps prevent a bottleneck that results if several hundreds of hosts connect to the vSphere Auto Deploy server simultaneously. After the boot operation is complete, hosts connect to vSphere Auto Deploy to complete the setup.

The stateful installs feature lets you provision hosts with the image profile over the network without having to set up the PXE boot infrastructure.

Introduction to Stateless Caching and Stateful Installs

You can use the System Cache Configuration host profile to provision hosts with vSphere Auto Deploy stateless caching and stateful installs.

Examples of Stateless Caching and Stateful Installs

Hosts provisioned with vSphere Auto Deploy cache the image (stateless caching)	Set up and apply a host profile for stateless caching. You can cache the image on a local disk, a remote disk, or a USB drive. Continue provisioning this host with vSphere Auto Deploy. If the vSphere Auto Deploy server becomes unavailable, for example because hundreds of hosts attempt to access it simultaneously, the host boots from the cache. The host attempts to reach the vSphere Auto Deploy server after the boot operation to complete configuration.
Hosts provisioned with vSphere Auto Deploy become stateful hosts	Set up and apply a host profile for stateful installs. When you provision a host with vSphere Auto Deploy, the image is installed on the local disk, a remote disk, or a USB drive. For subsequent boots, you boot from the disk. The host no longer uses vSphere Auto Deploy.

Preparation

To successfully use stateless caching or stateful installs, decide how to configure the system and set the boot order.

Table 18: Preparation for Stateless Caching or Stateful Installs

Requirement or Decision	Description
Decide on VMFS partition overwrite	When you install ESXi by using the interactive installer, you are prompted whether you want to overwrite an existing VMFS datastore. The System Cache Configuration host profile provides an option to overwrite existing VMFS partitions. The option is not available if you set up the host profile to use a USB drive.
Decide whether you need a highly available environment	If you use vSphere Auto Deploy with stateless caching, you can set up a highly available vSphere Auto Deploy environment to guarantee that virtual machines are migrated on newly provisioned hosts and that the environment supports vNetwork Distributed Switch even if the vCenter Server system becomes temporarily unavailable.
Set the boot order	The boot order you specify for your hosts depends on the feature you want to use.

Requirement or Decision	Description
	• To set up vSphere Auto Deploy with stateless caching, configure your host to first attempt to boot from the network, and to then attempt to boot from disk. If the vSphere Auto Deploy server is not available, the host boots using the cache. • To set up vSphere Auto Deploy for stateful installs on hosts that do not currently have a bootable disk, configure your hosts to first attempt to boot from disk, and to then attempt to boot from the network. **Note:** If you currently have a bootable image on the disk, configure the hosts for one-time PXE boot, and provision the host with vSphere Auto Deploy to use a host profile that specifies stateful installs.

Stateless Caching and Loss of Connectivity

If the ESXi hosts that run your virtual machines lose connectivity to the vSphere Auto Deploy server, the vCenter Server system, or both, some limitations apply the next time you reboot the host.

- If vCenter Server is available but the vSphere Auto Deploy server is unavailable, hosts do not connect to the vCenter Server system automatically. You can manually connect the hosts to the vCenter Server, or wait until the vSphere Auto Deploy server is available again.
- If both vCenter Server and vSphere Auto Deploy are unavailable, you can connect to each ESXi host by using the VMware Host Client, and add virtual machines to each host.
- If vCenter Server is not available, vSphere DRS does not work. The vSphere Auto Deploy server cannot add hosts to the vCenter Server. You can connect to each ESXi host by using the VMware Host Client, and add virtual machines to each host.
- If you make changes to your setup while connectivity is lost, the changes are lost when the connection to the vSphere Auto Deploy server is restored.

Understanding Stateless Caching and Stateful Installs

When you want to use vSphere Auto Deploy with stateless caching or stateful installs, you must set up a host profile, apply the host profile, and set the boot order.

When you apply a host profile that enables caching to a host, vSphere Auto Deploy partitions the specified disk. What happens next depends on how you set up the host profile and how you set the boot order on the host.

- vSphere Auto Deploy caches the image when you apply the host profile if **Enable stateless caching on the host** is selected in the System Cache Configuration host profile. No reboot is required. When you later reboot, the host continues to use the vSphere Auto Deploy infrastructure to retrieve its image. If the vSphere Auto Deploy server is not available, the host uses the cached image.
- vSphere Auto Deploy installs the image if **Enable stateful installs on the host** is selected in the System Cache Configuration host profile. When you reboot, the host initially boots using vSphere Auto Deploy to complete the installation. A reboot is then issued automatically, after which the host boots from disk, similar to a host that was provisioned with the installer. vSphere Auto Deploy no longer provisions the host.

You can apply the host profile from the vSphere Client, or write a vSphere Auto Deploy rule in a PowerCLI session that applies the host profile.

Using the vSphere Client to Set Up vSphere Auto Deploy for Stateless Caching or Stateful Installs

You can create a host profile on a reference host and apply that host profile to additional hosts or to a vCenter Server folder or cluster. The following workflow results.

1. You provision a host with vSphere Auto Deploy and edit that host's System Image Cache Configuration host profile.

2. You place one or more target hosts in maintenance mode, apply the host profile to each host, and instruct the host to exit maintenance mode.
3. What happens next depends on the host profile you selected.
   – If the host profile enabled stateless caching, the image is cached to disk. No reboot is required.
   – If the host profile enabled stateful installs, the image is installed. When you reboot, the host uses the installed image.

Using PowerCLI to Set Up vSphere Auto Deploy for Stateless Caching or Stateful Installs

You can create a host profile for a reference host and write a vSphere Auto Deploy rule that applies that host profile to other target hosts in a PowerCLI session. The following workflow results.

1. You provision a reference host with vSphere Auto Deploy and create a host profile to enable a form of caching.
2. You write a rule that provisions additional hosts with vSphere Auto Deploy and that applies the host profile of the reference host to those hosts.
3. vSphere Auto Deploy provisions each host with the image profile or by using the script bundle associated with the rule. The exact effect of applying the host profile depends on the host profile you selected.
   – For stateful installs, vSphere Auto Deploy proceeds as follows:
     • During first boot, vSphere Auto Deploy installs the image on the host.
     • During subsequent boots, the host boots from disk. The hosts do not need a connection to the vSphere Auto Deploy server.
   – For stateless caching, vSphere Auto Deploy proceeds as follows:
     • During first boot, vSphere Auto Deploy provisions the host and caches the image.
     • During subsequent boots, vSphere Auto Deploy provisions the host. If vSphere Auto Deploy is unavailable, the host boots from the cached image, however, setup can only be completed when the host can reach the vSphere Auto Deploy server.

Configure a Host Profile to Use Stateless Caching

When a host is set up to use stateless caching, the host uses a cached image if the vSphere Auto Deploy Server is not available. To use stateless caching, you must configure a host profile. You can apply that host profile to other hosts that you want to set up for stateless caching.

- Decide which disk to use for caching and determine whether the caching process will overwrite an existing VMFS partition.
- In production environments, protect the vCenter Server system and the vSphere Auto Deploy server by including them in a highly available environment. Having the vCenter Server in a management cluster guarantees that VDS and virtual machine migration are available. If possible, also protect other elements of your infrastructure. See Set Up Highly Available vSphere Auto Deploy Infrastructure.
- Set up your environment for vSphere Auto Deploy. See Preparing for vSphere Auto Deploy.
- Verify that a disk with at least 4GB of free space is available. If the disk is not yet partitioned, partitioning happens when you apply the host profile.
- Set up the host to attempt a network boot first and to boot from disk if network boot fails. See your hardware vendor's documentation.

- Create a host profile. See the *Host Profiles* documentation.

1. Navigate to **Home** > **Policies and Profiles** > **Host Profiles**.
2. Click the host profile you want to configure and select the **Configure** tab.
3. Click **Edit Host Profile**.
4. On the Edit host profile page of the wizard, select **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration**.
5. In the **System Image Cache Profile Settings** drop-down menu, choose a policy option.

Option	Description
Enable stateless caching on the host	Caches the image to disk.
Enable stateless caching to a USB disk on the host	Caches the image to a USB disk attached to the host.

6. Optional: If you select **Enable stateless caching on the host**, specify the information about the disk to use.

Option	Description
Arguments for first disk	When configuring a System Image Install disk, you have multiple options to define the device you want ESXi to be installed to and booted from. You can use the following arguments to define the disk for the installation: • `localesx` – The first disk detected containing a valid installation of ESXi • `local` – The first local disk detected by ESXi after boot • `remoteesx` - The first remote disk detected containing a valid installation of ESXi • `sortedremoteesx`- The first remote disk sorted by the lowest LUN ID detected containing a valid installation of ESXi • `remote` - The first remote disk detected by ESXi after boot • `sortedremote` - The first remote disk sorted by the lowest LUN ID detected by ESXi after boot • `device model` • `device vendor` • `vmkernel device driver name` You can get the values for the device model and vendor arguments by running the command `esxcli storage core device list` in a console to the ESXi host, logging in as the root. You get the vmkernel device driver name argument by running the command `esxcli storage core adapter list`. You must then identify the storage adapter to which your boot device is connected. By default, the system attempts to replace an existing ESXi installation, and then attempts to write to the local disk. You can use the **Arguments for first disk** field to specify a comma-separated list of disks to use, in order of preference. You can specify more than one disk. Use `localesx` for the first disk with ESX installed on it, model and vendor information, or specify the name of the vmkernel device driver. For example, to have the system first look for a disk with the model name ST3120814A, second for any disk that uses the mptsas driver, and third for the local disk, specify `ST3120814A,mptsas,local` as the value of this field. The first disk setting in the host profile specifies the search order for determining which disk to use for the cache. The search

Option	Description
	order is specified as a comma delimited list of values. The default setting `localesx,local` specifies that vSphere Auto Deploy should first look for an existing local cache disk. The cache disk is identified as a disk with an existing ESXi software image. If vSphere Auto Deploy cannot find an existing cache disk, it searches for an available local disk device. When searching for an available disk vSphere Auto Deploy uses the first empty disk that does not have an existing VMFS partition. You can use the first disk argument only to specify the search order. You cannot explicitly specify a disk. For example, you cannot specify a specific LUN on a SAN.
Check to overwrite any VMFS volumes on the selected disk	If you select this check box, the system overwrites existing VMFS volumes if not enough space is available to store the image, image profile, and host profile.
Check to ignore any SSD devices connected to the host	If you select this check box, the system ignores any existing SSD devices and does not store image profiles and host profiles on them.

7. Click **Save** to complete the host profile configuration.

Apply the host profile to individual hosts by using the Host Profiles feature in the vSphere Client. See the *Host Profiles* documentation. Alternatively, you can create a rule to assign the host profile to hosts with the vSphere Client or by using PowerCLI. See Write a Rule and Assign a Host Profile to Hosts.

- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.
- For hosts that are already provisioned with vSphere Auto Deploy, perform the test and repair compliance operations in a PowerCLI session, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the new host profile.

Configure a Host Profile to Enable Stateful Installs

To set up a host provisioned with vSphere Auto Deploy to boot from disk, you must configure a host profile. You can apply that host profile to other hosts that you want to set up for stateful installs.

- Decide which disk to use for storing the image, and determine whether the new image will overwrite an existing VMFS partition.
- Set up your environment for vSphere Auto Deploy. See Preparing for vSphere Auto Deploy.
- Verify that a disk with at least 4GB of free space is available. If the disk is not yet partitioned, partitioning happens when you apply the host profile.
- Set up the host to boot from disk. See your hardware vendor's documentation.

- Create a host profile. See the *Host Profiles* documentation.

You can configure the host profile on a single host. You can also create a host profile on a reference host and apply that host profile to other hosts.

1. Navigate to **Home** > **Policies and Profiles** > **Host Profiles**.
2. Click the host profile you want to configure and select the **Configure** tab.
3. Click **Edit Host Profile**.
4. On the Edit host profile page of the wizard, select **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration**.
5. In the **System Image Cache Profile Settings** drop-down menu, choose a policy option.

Option	Description
Enable stateful installs on the host	Caches the image to a disk.
Enable stateful installs to a USB disk on the host	Caches the image to a USB disk attached to the host.

6. Optional: If you select **Enable stateful installs on the host**, specify information about the disk to use.

Option	Description
Arguments for first disk	When configuring a System Image Install disk, you have multiple options to define the device you want ESXi to be installed to and booted from. You can use the following arguments to define the disk for the installation: • `localesx` – The first disk detected containing a valid installation of ESXi • `local` – The first local disk detected by ESXi after boot • `remoteesx` - The first remote disk detected containing a valid installation of ESXi • `sortedremoteesx`- The first remote disk sorted by the lowest LUN ID detected containing a valid installation of ESXi • `remote` - The first remote disk detected by ESXi after boot • `sortedremote` - The first remote disk sorted by the lowest LUN ID detected by ESXi after boot • `device model` • `device vendor` • `vmkernel device driver name` You can get the values for the device model and vendor arguments by running the command `esxcli storage core device list` in a console to the ESXi host, logging in as the root. You get the vmkernel device driver name argument by running the command `esxcli storage core adapter list`. You must then identify the storage adapter to which your boot device is connected. By default, the system attempts to replace an existing ESXi installation, and then attempts to write to the local disk. You can use the **Arguments for first disk** field to specify a comma-separated list of disks to use, in order of preference. You can specify more than one disk. Use `localesx` for the first disk with ESX installed on it, model and vendor information, or specify the name of the vmkernel device driver. For example, to have the system first look for a disk with the model name ST3120814A, second for any disk that

Option	Description
	uses the mptsas driver, and third for the local disk, specify `ST3120814A,mptsas,local` as the value of this field. The first disk setting in the host profile specifies the search order for determining which disk to use for the cache. The search order is specified as a comma delimited list of values. The default setting `localesx,local` specifies that vSphere Auto Deploy should first look for an existing local cache disk. The cache disk is identified as a disk with an existing ESXi software image. If vSphere Auto Deploy cannot find an existing cache disk, it searches for an available local disk device. When searching for an available disk vSphere Auto Deploy uses the first empty disk that does not have an existing VMFS partition. You can use the first disk argument only to specify the search order. You cannot explicitly specify a disk. For example, you cannot specify a specific LUN on a SAN.
Check to overwrite any VMFS volumes on the selected disk	If you select this check box, the system overwrites existing VMFS volumes if not enough space is available to store the image, image profile, and host profile.
Check to ignore any SSD devices connected to the host	If you select this check box, the system ignores any existing SSD devices and does not store image profiles and host profiles on them.

7. Click **Save** to complete the host profile configuration.

Apply the host profile to individual hosts by using the Host Profiles feature in the vSphere Client. See the *Host Profiles* documentation. Alternatively, you can create a rule to assign the host profile to hosts with the vSphere Client or by using PowerCLI. See Write a Rule and Assign a Host Profile to Hosts.

- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.
- For hosts that are already provisioned with vSphere Auto Deploy, perform the test and repair compliance operations in a PowerCLI session, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the new host profile.

Setting Up a vSphere Auto Deploy Reference Host

In an environment where no state is stored on the ESXi host, a reference host helps you set up multiple hosts with the same configuration.

You configure the reference host with the logging, coredump, and other settings that you want, save the host profile, and write a rule that applies the host profile to other hosts as needed. You can configure the storage, networking, and security settings on the reference host and set up services such as syslog and NTP.

Understanding Reference Host Setup

A well-designed reference host connects to all services such as syslog, NTP, and so on. The reference host setup might also include security, storage, networking, and ESXi Dump Collector. You can apply such a host's setup to other hosts by using host profiles.

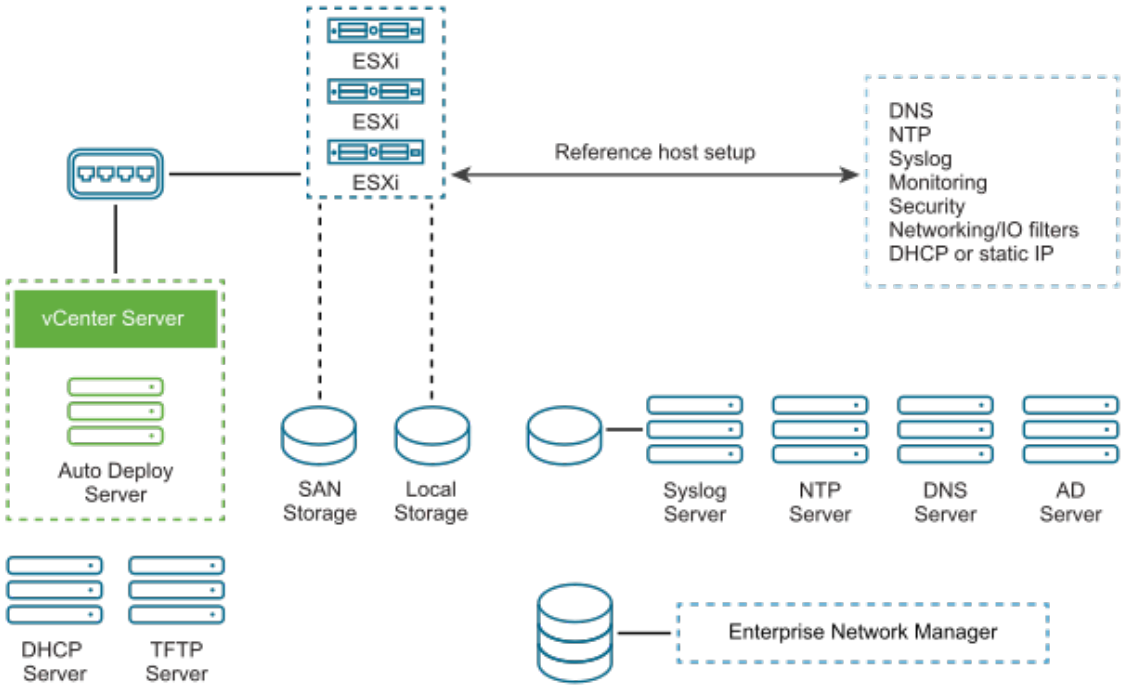
The exact setup of your reference host depends on your environment, but you might consider the following customization.

NTP Server Setup	When you collect logging information in large environments, you must make sure that log times are coordinated. Set up the reference host to use the NTP server in your environment that all hosts can share. You can specify an NTP server by running the `esxcli system ntp set` command. You can start and stop

	the NTP service for a host with the `esxcli system ntp set` command, or the vSphere Client.
Syslog Server Setup	All ESXi hosts run a syslog service (`vmsyslogd`), which logs messages from the VMkernel and other system components to a file. You can specify the log host and manage the log location, rotation, size, and other attributes by running the `esxcli system syslog` command or by using the vSphere Client. Setting up logging on a remote host is especially important for hosts provisioned with vSphere Auto Deploy that have no local storage. You can optionally install VMware vCenter Log Insight, which provides log aggregation and analytics.
Core Dump Setup	You can set up your reference host to send core dumps to a shared SAN LUN, or you can install ESXi Dump Collector in your environment and configure the reference host to use ESXi Dump Collector. See Configure ESXi Dump Collector with ESXCLI . You can either install ESXi Dump Collector by using the vCenter Server installation media or use the ESXi Dump Collector that is included in vCenter Server. After setup is complete, VMkernel memory is sent to the specified network server when the system encounters a critical failure.
Security Setup	In most deployments, all hosts that you provision with vSphere Auto Deploy must have the same security settings. You can, for example, set up the firewall to allow certain services to access the ESXi system, set up the security configuration, user configuration, and user group configuration for the reference host with the vSphere Client or with ESXCLI commands. Security setup includes shared user access settings for all hosts. You can achieve unified user access by setting up your reference host to use Active Directory. See the *vSphere Security* documentation. **Note:** If you set up Active Directory by using host profiles, the passwords are not protected. Use the vSphere Authentication Service to set up Active Directory to avoid exposing the Active Directory password.
Networking and Storage Setup	If you reserve a set of networking and storage resources for use by hosts provisioned with vSphere Auto Deploy, you can set up your reference host to use those resources.

In large deployments, the reference host setup supports an Enterprise Network Manager, which collects all information coming from the different monitoring services that are running in the environment.

Figure 9: vSphere Auto Deploy Reference Host Setup



Options for Configuration of a vSphere Auto Deploy Reference Host explains how to perform this setup.

Watch the video "Auto Deploy Reference Hosts" for information about the reference host setup:

Options for Configuration of a vSphere Auto Deploy Reference Host

You can configure a reference host by using the vSphere Client, ESXCLI, or host profiles.

To set up a reference host, you can use the approach that suits you best.

vSphere Client	The vSphere Client supports setup of networking, storage, security, and most other aspects of an ESXi host. Set up your environment and create a host profile from the reference host for use by vSphere Auto Deploy.
ESXCLI	You can use ESXCLI for setup of many aspects of your host. ESXCLI is suitable for configuring many of the services in the vSphere environment. Commands include `esxcli system ntp` for setting up an NTP server, `esxcli system syslog` for setting up a syslog server, `esxcli network route` for adding routes and set up the default route, and `esxcli system coredump` for configuring ESXi Dump Collector.
Host Profiles Feature	Best practice is to set up a host with vSphere Client or ESXCLI and create a host profile from that host. You can instead use the Host Profiles feature in the vSphere Client and save that host profile.

vSphere Auto Deploy applies all common settings from the host profile to all target hosts. If you set up the host profile to prompt for user input, all hosts provisioned with that host profile come up in maintenance mode. You must reapply the host profile or reset host customizations to be prompted for the host-specific information.

Related Links

Configure ESXi Dump Collector with ESXCLI on page 1102
Hosts provisioned with vSphere Auto Deploy do not have a local disk to store core dumps on. You can configure ESXi Dump Collector by using ESXCLI commands and keep core dumps on a network server for use during debugging.

Configure ESXi Dump Collector from the Host Profiles Feature in the vSphere Client on page 1103
Hosts provisioned with vSphere Auto Deploy do not have a local disk to store core dumps on. You can configure a reference host to use ESXi Dump Collector by using the Host Profiles feature in the vSphere Client.

Configure Syslog from the Host Profiles Feature in the vSphere Client on page 1103
Hosts provisioned with vSphere Auto Deploy usually do not have sufficient local storage to save system logs. You can specify a remote syslog server for those hosts by setting up a reference host, saving the host profile, and applying that host profile to other hosts as needed.

Enable NTP Client on a Reference Host in the vSphere Client on page 1104
When you collect logging information in large environments, you must ensure that log times are coordinated. You can set up the reference host to use the NTP server in your environment, extract the host profile and create a vSphere Auto Deploy rule to apply it to other hosts.

Configure Networking for Your vSphere Auto Deploy Host in the vSphere Client on page 1104
You can set up networking for your vSphere Auto Deploy reference host and apply the host profile to all other hosts to guarantee a fully functional networking environment.

Configure a Reference Host for Auto-Partitioning on page 1105
By default, vSphere Auto Deploy provisions hosts only if a partition is available on the host. The auto-partitioning option creates a VMFS datastore on your host's local storage. You can set up a reference host to auto-partition all hosts that you provision with vSphere Auto Deploy.

Configure ESXi Dump Collector with ESXCLI

Hosts provisioned with vSphere Auto Deploy do not have a local disk to store core dumps on. You can configure ESXi Dump Collector by using ESXCLI commands and keep core dumps on a network server for use during debugging.

Install ESXCLI if you want to configure the host to use ESXi Dump Collector. In troubleshooting situations, you can use ESXCLI in the ESXi Shell instead.

A core dump is the state of working memory if there is host failure. By default, a core dump is saved to the local disk. ESXi Dump Collector is especially useful for vSphere Auto Deploy, but is supported for any ESXi host. ESXi Dump Collector supports other customization, including sending core dumps to the local disk and is included with the vCenter Server management node.

Note: ESXi Dump Collector is not supported to be configured on a VMkernel interface that is running on a NSX-T N-VDS switch.

If you intend to use IPv6, and if both the ESXi host and ESXi Dump Collector are on the same local link, both can use either local link scope IPv6 addresses or global scope IPv6 addresses.

If you intend to use IPv6, and if ESXi and ESXi Dump Collector are on different hosts, both require global scope IPv6 addresses. The traffic routes through the default IPv6 gateway.

1. Set up an ESXi system to use ESXi Dump Collector by running `esxcli system coredump` in the local ESXi Shell or by using ESXCLI.

   ```
   esxcli system coredump network set --interface-name vmk0 --server-ip 10xx.xx.xx.xx --server-port 6500
   ```

   You must specify a VMkernel NIC and the IP address and optional port of the server to send the core dumps to. You can use an IPv4 address or an IPv6 address. If you configure an ESXi system that is running on a virtual machine that is using a vSphere standard switch, you must select a VMkernel port that is in promiscuous mode.

2. Enable ESXi Dump Collector.

   ```
   esxcli system coredump network set --enable true
   ```

3. Optional: Verify that ESXi Dump Collector is configured correctly.
   ```
   esxcli system coredump network check
   ```

The host on which you have set up ESXi Dump Collector is configured to send core dumps to the specified server by using the specified VMkernel NIC and optional port.

- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.
- For hosts that are already provisioned with vSphere Auto Deploy, perform the test and repair compliance operations in a PowerCLI session, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the new host profile.

Configure ESXi Dump Collector from the Host Profiles Feature in the vSphere Client

Hosts provisioned with vSphere Auto Deploy do not have a local disk to store core dumps on. You can configure a reference host to use ESXi Dump Collector by using the Host Profiles feature in the vSphere Client.

- Verify that you have created the host profile on which you want to configure a coredump policy. For more information on how to create a host profile, see the *vSphere Host Profiles* documentation.
- Verify that at least one partition has sufficient storage capability for core dumps from multiple hosts provisioned with vSphere Auto Deploy.

Best practice is to set up hosts to use ESXi Dump Collector with the `esxcli system coredump` command and save the host profile. For more information, see Configure ESXi Dump Collector with ESXCLI .

1. Navigate to **Home** > **Policies and Profiles** > **Host Profiles**.
2. Click the host profile you want to configure and select the **Configure** tab.
3. Click **Edit Host Profile**.
4. Select **Networking Configuration** > **Network Coredump Settings**.
5. Select the **Enabled** check box.
6. Specify the host NIC to use, the Network Coredump Server IP, and the Network Coredump Server Port.
7. Click **Save** to complete the host profile configuration.

- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.
- For hosts that are already provisioned with vSphere Auto Deploy, perform the test and repair compliance operations in a PowerCLI session, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the new host profile.

Configure Syslog from the Host Profiles Feature in the vSphere Client

Hosts provisioned with vSphere Auto Deploy usually do not have sufficient local storage to save system logs. You can specify a remote syslog server for those hosts by setting up a reference host, saving the host profile, and applying that host profile to other hosts as needed.

- If you intend to use a remote syslog host, set up that host before you customize host profiles.

- Verify that you have access to the vSphere Client and the vCenter Server system.

Best practice is to set up the syslog server on the reference host with the vSphere Client or the `esxcli system syslog` command and to save the host profile. You can also set up syslog from the Host Profiles feature in the vSphere Client.

1. Navigate to **Home** > **Policies and Profiles** > **Host Profiles**.
2. Optional: If no reference host exists in your environment, click **Extract Profile from Host** to create a host profile.
3. Click the host profile you want to configure and select the **Configure** tab.
4. Click **Edit Host Profile**.
5. Select **Advanced Configuration Settings** > **Advanced Options** > **Advanced configuration options**.
   You can select specific sub-profiles and edit the syslog settings.
6. Optional: To create an advanced configuration option.
   a) Click the **Add sub-profile** icon.
   b) From the **Advanced option** drop-down list select **Configure a fixed option**.
   c) Specify *Syslog.global.loghost* as the name of the option, and your host as the value of the option.
7. Click **Save** to complete the host profile configuration.

- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.
- For hosts that are already provisioned with vSphere Auto Deploy, perform the test and repair compliance operations in a PowerCLI session, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the new host profile.

Enable NTP Client on a Reference Host in the vSphere Client
When you collect logging information in large environments, you must ensure that log times are coordinated. You can set up the reference host to use the NTP server in your environment, extract the host profile and create a vSphere Auto Deploy rule to apply it to other hosts.

1. Navigate to **Home** > **Hosts and Clusters**, and select an ESXi host that you want to use as a reference host.
2. Select the **Configure** tab.
3. Under **System**, select **Time Configuration** and click **Edit**.
4. Select the **Use Network Time Protocol (Enable NTP client)** radio button.
   This option synchronizes the time and date of the host with an NTP server. The NTP service on the host periodically takes the time and date from the NTP server.
5. From the **NTP Service Startup Policy** drop-down list, select **Start and stop with host**.
6. In the **NTP Servers** text box, type the IP addresses or host names of the NTP servers that you want to use.
7. Click **OK**.

- Extract a host profile from the reference host. See the *Host Profiles* documentation.
- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.

Configure Networking for Your vSphere Auto Deploy Host in the vSphere Client
You can set up networking for your vSphere Auto Deploy reference host and apply the host profile to all other hosts to guarantee a fully functional networking environment.

Provision the host you want to use as your reference host with an ESXi image by using vSphere Auto Deploy.

1. Navigate to **Home** > **Hosts and Clusters**, and select an ESXi host that you want to use as a reference host.
2. Select the **Configure** tab and navigate to **Networking**.
3. Perform the networking setup.
   If you are using virtual switches and not vSphere Distributed Switch, do not add other VMkernel NICs to vSwitch0.
4. After the reference host is configured, reboot the system to verify that vmk0 is connected to the Management Network.
5. If no host profile exists for your reference host, create a host profile.

- Create a rule that applies the host profile to all hosts that you want to provision with the settings specified in the reference host. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.
- For hosts that are already provisioned with vSphere Auto Deploy, perform the test and repair compliance operations in a PowerCLI session, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the new host profile.

Configure a Reference Host for Auto-Partitioning
By default, vSphere Auto Deploy provisions hosts only if a partition is available on the host. The auto-partitioning option creates a VMFS datastore on your host's local storage. You can set up a reference host to auto-partition all hosts that you provision with vSphere Auto Deploy.

- Provision the host that you want to use as your reference host with an ESXi image by using vSphere Auto Deploy.
- Verify that you have access to a vSphere Client that can connect to the vCenter Server system.

CAUTION: If you change the default auto-partitioning behavior, vSphere Auto Deploy overwrites existing partitions regardless of their content. If you turn on this option, ensure that no unintended data loss results.

To ensure that local SSDs remain unpartitioned during auto-partitioning, you must set the parameter `skipPartitioningSsds=TRUE` on the reference host.

For more information about preventing SSD formatting during auto-partitioning, see the *vSphere Storage* documentation.

1. Navigate to **Home** > **Hosts and Clusters**, and select an ESXi host that you want to use as a reference host.
2. Select the **Configure** tab.
3. Under **System**, select **Advanced System Settings** and click **Edit**.
4. Search for the `VMkernel.Boot.autoPartition` key and set the value to **true**.
5. Optional: If you want the local SSDs to remain unpartitioned, search for the `VMkernel.Boot.skipPartitioningSsds` key and set the value to **true**.
6. Click **OK**.
7. If no host profile exists for your reference host, create a host profile.

Auto-partitioning is performed when the hosts boot.

- Use vSphere Auto Deploy to create a rule that applies the host profile of your reference host to all hosts immediately when they boot. To create a rule with the vSphere Client, see Create a Deploy Rule. For writing a rule in a PowerCLI session, see Write a Rule and Assign a Host Profile to Hosts.

Converting Stateless Hosts to Stateful Hosts

You can add physical storage to your stateless ESXi, convert them to stateful ESXi hosts, and add the hosts to a cluster that you manage by an image.

Your ESXi hosts must have physical storage attached, because a cluster managed by an image does not support stateless ESXi hosts, that use a Preboot Execution Environment (PXE) boot.

To ensure that image components are installed on a physical disk of an ESXi host during a boot process, Auto Deploy verifies that a host profile is part of the PXE boot image. The host profile must contain a "System Image Cache Profile Settings" policy with configuration set to "Enable stateful installs on the host" or "Enable stateful installs to a USB disk on the host". If the attached host profile does not contain this policy or the policy's configuration differs, then the policy is automatically configured to support a stateful installation. If a host profile is missing, a new host profile is attached to the cluster, containing only the "System Image Cache Profile Settings" policy with a configuration for a stateful installation.

Convert a Diskless ESXi Host

To convert your diskless ESXi hosts to a cluster managed by an image, you must first convert these hosts to stateful hosts by adding physical storage and installing an ESXi7.0 image.

- Prepare your system and install the Auto Deploy Server. For more information, see *Prepare Your System for vSphere Auto Deploy* in the *VMware ESXi Installation and Setup* documentation.
- The ESXi host is booting from an Auto Deploy rule that contains an Image Profile.
- The Auto Deploy service is running.
- You have a USB stick or other supported storage.

For information on stateless caching and stateful installs, see Use vSphere Auto Deploy for Stateless Caching and Stateful Installs.

1. From the home menu, click **Policies and Profiles**, and select **Host Profiles**.
2. Extract a host profile from a running ESXi host or duplicate an existing host profile with a specified configuration and a host location.

   The existing host profile can be attached either to a host or to a cluster.
3. Right-click the new host profile, select **Edit Host Profile**, and browse to **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration**.
4. Select **Enable stateful installs to a USB disk on the host** from the drop-down menu.

   If other supported storage is used, select the **Enable stateful installs on the host** from the drop-down menu, enter arguments for the first disk, and select the check boxes if needed.
5. If you duplicated an existing host profile and the host profile was attached to a cluster, attach the new host profile to the cluster.
6. From the home menu, click **Auto Deploy**.
7. Deactivate the Auto Deploy rule that contains an Image Profile, and click **Edit**.

   The Edit Deploy Rule dialog box appears.
8. On the **Select image profile** page of the wizard, select an ESXi 7.0 image profile.
9. On the **Select host profile** page of the wizard, select the new host profile.
10. Activate the rule and move the rule to the rule's initial position in the ordered list.
11. On the **Deployed Hosts** tab, select a single or multiple ESXi hosts.
12. Click **Remediate Host Associations** for the ESXi host.

    You can monitor the progress of the remediation process in the Recent Tasks pane.
13. Shut down the remediated ESXi hosts.
14. After the ESXi hosts are powered off, install the USB sticks or other supported storage as local boot disks.

    The USB sticks or other supported storage must be empty.

15. Power on each ESXi host, enter the BIOS/UEFI setup, and change the boot order to boot first from the newly added storage and then from the network.

    Since the newly added storage is empty, each ESXi host boots from the network and installs the ESXi 7.0 image that you specified earlier on the storage. After the installation, each ESXi host reboots and boots from the newly added storage.

The ESXi hosts boot by default from the new storage and operate as if the ESXi7.0 image is installed from a standard DVD.

Add the ESXi hosts to a cluster that you manage by a single image. For more information, see *Add a Host* from the *vCenter Server and Host Management* documentation.

Convert a Stateless ESXi Host with Enabled Stateless Caching

To add your stateless ESXi hosts to a cluster that you manage by an image, you must first convert the hosts to stateful hosts by installing a standard ESXi 7.0 image.

- Prepare your system and install the Auto Deploy Server. For more information, see *Prepare Your System for vSphere Auto Deploy* in the *VMware ESXi Installation and Setup* documentation.
- The ESXi host is booting from an Auto Deploy rule that contains an Image Profile.
- The Auto Deploy service is running.

For information on stateless caching and stateful installs, see Use vSphere Auto Deploy for Stateless Caching and Stateful Installs.

1. From the home menu, click **Policies and Profiles**, and select **Host Profiles**.
2. Extract a host profile from a running ESXi host or duplicate an existing host profile with a specified configuration and a host location.

   The existing host profile can be attached either to a host or to a cluster.
3. Right-click the new host profile, select **Edit Host Profile**, and browse to **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration**.
4. Select **Enable stateful installs on the host** from the drop-down menu, enter `local` in the **Arguments for first disk** text box, and select the **Check to overwrite any VMFS volumes on the selected disk** check box.
5. If you duplicated an existing host profile and the host profile was attached to a cluster, attach the new host profile to the cluster.
6. From the home menu, click **Auto Deploy**.
7. Deactivate the Auto Deploy rule that contains an Image Profile, and click **Edit**.

   The Edit Deploy Rule dialog box appears.
8. On the **Select image profile** page of the wizard, select an ESXi 7.0 image profile.
9. On the **Select host profile** page of the wizard, select the new host profile.
10. Activate the rule and move the rule to the rule's initial position in the ordered list.
11. On the **Deployed Hosts** tab, select a single or multiple ESXi hosts.
12. Click **Remediate Host Associations** for the ESXi host.

    You can monitor the progress of the remediation process in the Recent Tasks pane.
13. Restart the ESXi hosts.

    If an ESXi host has a legacy BIOS, you can change the boot order in the BIOS setup to first to boot from the local storage. For UEFI-based ESXi hosts the boot order changes automatically during the reboot.

    Each ESXi host boots from the network and installs the ESXi7.0 image that you specified earlier on the storage used previously for caching. After the installation, each ESXi host reboots again and boots from the local storage.

The ESXi hosts boot by default from the new storage and operate as if the ESXi7.0 image is installed from a standard DVD.

Add the ESXi hosts to a cluster that you manage by a single image. For more information, see *Add a Host* from the *vCenter Server and Host Management* documentation.

Convert a Stateless ESXi Host with a Single VMFS Partition on the Local Disk

To add your stateless ESXi hosts to a cluster that you manage by an image, you must first convert the hosts to stateful hosts by repartitioning the VMFS partitions and installing a standard ESXi7.0 image.

- Prepare your system and install the Auto Deploy Server. For more information, see *Prepare Your System for vSphere Auto Deploy* in the *VMware ESXi Installation and Setup* documentation.
- The ESXi host is booting from an Auto Deploy rule that contains an Image Profile.
- The Auto Deploy service is running.

For information on stateless caching and stateful installs, see Use vSphere Auto Deploy for Stateless Caching and Stateful Installs.

1. From the home menu, click **Policies and Profiles**, and select **Host Profiles**.
2. Extract a host profile from a running ESXi host or duplicate an existing host profile with a specified configuration and a host location.

   The existing host profile can be attached either to a host or to a cluster.
3. Right-click the new host profile, select **Edit Host Profile**, and browse to **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration**.
4. Select **Enable stateful installs on the host** from the drop-down menu, enter `localesx` in the **Arguments for first disk** text box.
5. If you duplicated an existing host profile and the host profile was attached to a cluster, attach the new host profile to the cluster.
6. From the home menu, click **Auto Deploy**.
7. Deactivate the Auto Deploy rule that contains an Image Profile, and click **Edit**.

   The Edit Deploy Rule dialog box appears.
8. On the **Select image profile** page of the wizard, select an ESXi 7.0 image profile.
9. On the **Select host profile** page of the wizard, select the new host profile.
10. Activate the rule and move the rule to the rule's initial position in the ordered list.
11. On the **Deployed Hosts** tab, select a single or multiple ESXi hosts.
12. Click **Remediate Host Associations** for the ESXi host.

    You can monitor the progress of the remediation process in the Recent Tasks pane.
13. Restart the ESXi hosts.

    If an ESXi host has a legacy BIOS, you can change the boot order in the BIOS setup to first to boot from the local storage. For UEFI-based ESXi hosts the boot order changes automatically during the reboot.

    Each ESXi host boots from the network, repartitions the VMFS partition to a standard ESXi installation partition, and installs the ESXi7.0 image that you specified earlier on the partition. After the installation, each ESXi host reboots again and boots from the standard ESXi partition.

The ESXi hosts boot by default from the new partition and operate as if the ESXi7.0 image is installed from a standard DVD.

Add the ESXi hosts to a cluster that you manage by a single image. For more information, see *Add a Host* from the *vCenter Server and Host Management* documentation.

Convert a Stateless ESXi Host with a Single VMFS Partition on a Remote Disk
To add your stateless ESXi hosts to a cluster that you manage by an image, first you must convert the hosts to stateful hosts by repartitioning their remote VMFS partitions and installing a standard ESXi7.0 image. For example, your ESXi host can boot from Fibre Channel SAN or from iSCSI SAN.

- Prepare your system and install the Auto Deploy Server. For more information, see *Prepare Your System for vSphere Auto Deploy* in the *VMware ESXi Installation and Setup* documentation.
- The ESXi host is booting from an Auto Deploy rule that contains an Image Profile.
- The Auto Deploy service is running.

For information on stateless caching and stateful installs, see Use vSphere Auto Deploy for Stateless Caching and Stateful Installs.

For more information on booting from a remote disk, see the *Booting from iSCSI SAN* in the *vSphere Storage* documentation.

1. From the home menu, click **Policies and Profiles**, and select **Host Profiles**.
2. Extract a host profile from a running ESXi host or duplicate an existing host profile with a specified configuration and a host location.

   The existing host profile can be attached either to a host or to a cluster.
3. Right-click the new host profile, select **Edit Host Profile**, and browse to **Advanced Configuration Settings** > **System Image Cache Configuration** > **System Image Cache Configuration**.
4. Select **Enable stateful installs on the host** from the drop-down menu, enter `remoteesx,remote` or `sortedremoteesx,sortedremote` in the **Arguments for first disk** text box.
5. If you duplicated an existing host profile and the host profile was attached to a cluster, attach the new host profile to the cluster.
6. From the home menu, click **Auto Deploy**.
7. Deactivate the Auto Deploy rule that contains an Image Profile, and click **Edit**.

   The Edit Deploy Rule dialog box appears.
8. On the **Select image profile** page of the wizard, select an ESXi 7.0 image profile.
9. On the **Select host profile** page of the wizard, select the new host profile.
10. Activate the rule and move the rule to the rule's initial position in the ordered list.
11. On the **Deployed Hosts** tab, select a single or multiple ESXi hosts.
12. Click **Remediate Host Associations** for the ESXi host.

    You can monitor the progress of the remediation process in the Recent Tasks pane.
13. Restart the ESXi hosts.

    Each ESXi host boots from the network, repartitions the VMFS partition to a standard ESXi installation partition, and installs the ESXi7.0 image that you specified earlier on the partition. After the installation, each ESXi host reboots again and boots from the remote standard ESXi partition.

The ESXi hosts boot by default from the new partition and operate as if the ESXi7.0 image is installed from a standard DVD.

Add the ESXi hosts to a cluster that you manage by a single image. For more information, see *Add a Host* from the *vCenter Server and Host Management* documentation.

vSphere Auto Deploy Best Practices

Set up a highly available vSphere Auto Deploy infrastructure in large production environments or when using stateless caching.

Follow best practices when installing vSphere Auto Deploy and when using vSphere Auto Deploy with other vSphere components. Set up a highly available vSphere Auto Deploy infrastructure in large production environments or when using stateless caching. Follow all security guidelines that you would follow in a PXE boot environment, and consider the recommendations in this chapter.

vSphere Auto Deploy Best Practices

Follow vSphere Auto Deploy best practices to set up networking, configure vSphere HA, and optimize your environment for vSphere Auto Deploy.

See the VMware Knowledge Base for additional best practice information.

vSphere Auto Deploy and vSphere HA Best Practices

You can improve the availability of the virtual machines running on hosts provisioned with vSphere Auto Deploy by following best practices.

Some environments configure the hosts provisioned with vSphere Auto Deploy with a distributed switch or configure virtual machines running on the hosts with Auto Start Manager. In such environments, deploy the vCenter Server system so that its availability matches the availability of the vSphere Auto Deploy server. Several approaches are possible.

- Deploy vCenter Server. The vSphere Auto Deploy server is included.
- Run vCenter Server in a vSphere HA enabled cluster and configure the virtual machine with a vSphere HA restart priority of high. Include two or more hosts in the cluster that are not managed by vSphere Auto Deploy and pin the vCenter Server virtual machine to these hosts by using a rule (vSphere HA DRS required VM to host rule). You can set up the rule and then deactivate DRS if you do not want to use DRS in the cluster. The greater the number of hosts that are not managed by vSphere Auto Deploy, the greater your resilience to host failures.

  Note: This approach is not suitable if you use Auto Start Manager. Auto Start Manager is not supported in a cluster enabled for vSphere HA.

vSphere Auto Deploy Networking Best Practices

Prevent networking problems by following vSphere Auto Deploy networking best practices.

vSphere Auto Deploy and IPv6	Because vSphere Auto Deploy takes advantage of the iPXE infrastructure, if the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, the vSphere Auto Deploy server must have an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.
IP Address Allocation	Use DHCP reservations for address allocation. Fixed IP addresses are supported by the host customization mechanism, but providing input for each host is not recommended.
VLAN Considerations	Use vSphere Auto Deploy in environments that do not use VLANs. If you intend to use vSphere Auto Deploy in an environment that uses VLANs, make sure that the hosts that you want to provision can reach the DHCP server. How hosts are assigned to a VLAN depends on the setup at your site. The VLAN ID might be assigned by the switch or the router, or might be set in the host's BIOS or through the host profile. Contact your network

administrator to determine the steps for allowing hosts to reach the DHCP server.

vSphere Auto Deploy and VMware Tools Best Practices

When you provision hosts with vSphere Auto Deploy, you can select an image profile that includes VMware Tools, or select the smaller image associated with the image profile that does not contain VMware Tools.

You can download two image profiles from the VMware download site.

- *xxxxx*-standard: An image profile that includes the VMware Tools binaries, required by the guest operating system running inside a virtual machine. The image is usually named esxi-*version*-*xxxxx*-standard.
- *xxxxx*-no-tools: An image profile that does not include the VMware Tools binaries. This image profile is usually smaller has a lower memory overhead, and boots faster in a PXE-boot environment. This image is usually named esxi-*version*-*xxxxx*-no-tools.

You can deploy ESXi using either image profile.

- If the network boot time is of no concern, and your environment has sufficient extra memory and storage overhead, use the image that includes VMware Tools.
- If you find the network boot time too slow when using the standard image, or if you want to save some space on the hosts, you can use the image profile that does not include VMware Tools, and place the VMware Tools binaries on shared storage. See, Provision ESXi Host by Using an Image Profile Without VMware Tools.

vSphere Auto Deploy Load Management Best Practices

Simultaneously booting large numbers of hosts places a significant load on the vSphere Auto Deploy server. Because vSphere Auto Deploy is a Web server at its core, you can use existing Web server scaling technologies to help distribute the load. For example, one or more caching reverse proxy servers can be used with vSphere Auto Deploy. The reverse proxies serve up the static files that make up the majority of an ESXi boot image. Configure the reverse proxy to cache static content and pass all requests through to the vSphere Auto Deploy server. For more information, watch the video "Using Reverse Web Proxy Servers for vSphere Auto Deploy Scalability":

Use multiple TFTP servers to point to different proxy servers. Use one TFTP server for each reverse proxy server. After that, set up the DHCP server to send different hosts to different TFTP servers.

When you boot the hosts, the DHCP server redirects them to different TFTP servers. Each TFTP server redirects hosts to a different server, either the vSphere Auto Deploy server or a reverse proxy server, significantly reducing the load on the vSphere Auto Deploy server.

After a massive power outage, bring up the hosts on a per-cluster basis. If you bring multiple clusters online simultaneously, the vSphere Auto Deploy server might experience CPU bottlenecks. All hosts might come up after a delay. The bottleneck is less severe if you set up the reverse proxy.

vSphere Auto Deploy Logging and Troubleshooting Best Practices

To resolve problems that you encounter with vSphere Auto Deploy, use the vSphere Auto Deploy logging information from the vSphere Client and set up your environment to send logging information and core dumps to remote hosts.

vSphere Auto Deploy Logs	Download the vSphere Auto Deploy logs by going to the vSphere Auto Deploy page in the vSphere Client. See, Download vSphere Auto Deploy Logs.
Setting Up Syslog	Set up a remote syslog server. See the *vCenter Server and Host Management* documentation for syslog server configuration information. Configure the first host you boot to use the remote

	syslog server and apply that host's host profile to all other target hosts. Optionally, install and use the vSphere Syslog Collector, a vCenter Server support tool that provides a unified architecture for system logging, enables network logging, and lets you combine logs from multiple hosts.
Setting Up ESXi Dump Collector	Hosts provisioned with vSphere Auto Deploy do not have a local disk to store core dumps on. Install ESXi Dump Collector and set up your first host so that all core dumps are directed to ESXi Dump Collector, and apply the host profile from that host to all other hosts. See Configure ESXi Dump Collector with ESXCLI .

Using vSphere Auto Deploy in a Production Environment

When you move from a proof of concept setup to a production environment, take care to make the environment resilient.

- Protect the vSphere Auto Deploy server. See vSphere Auto Deploy and vSphere HA Best Practices.
- Protect all other servers in your environment, including the DHCP server and the TFTP server.
- Follow VMware security guidelines, including those outlined in vSphere Auto Deploy Security Considerations.

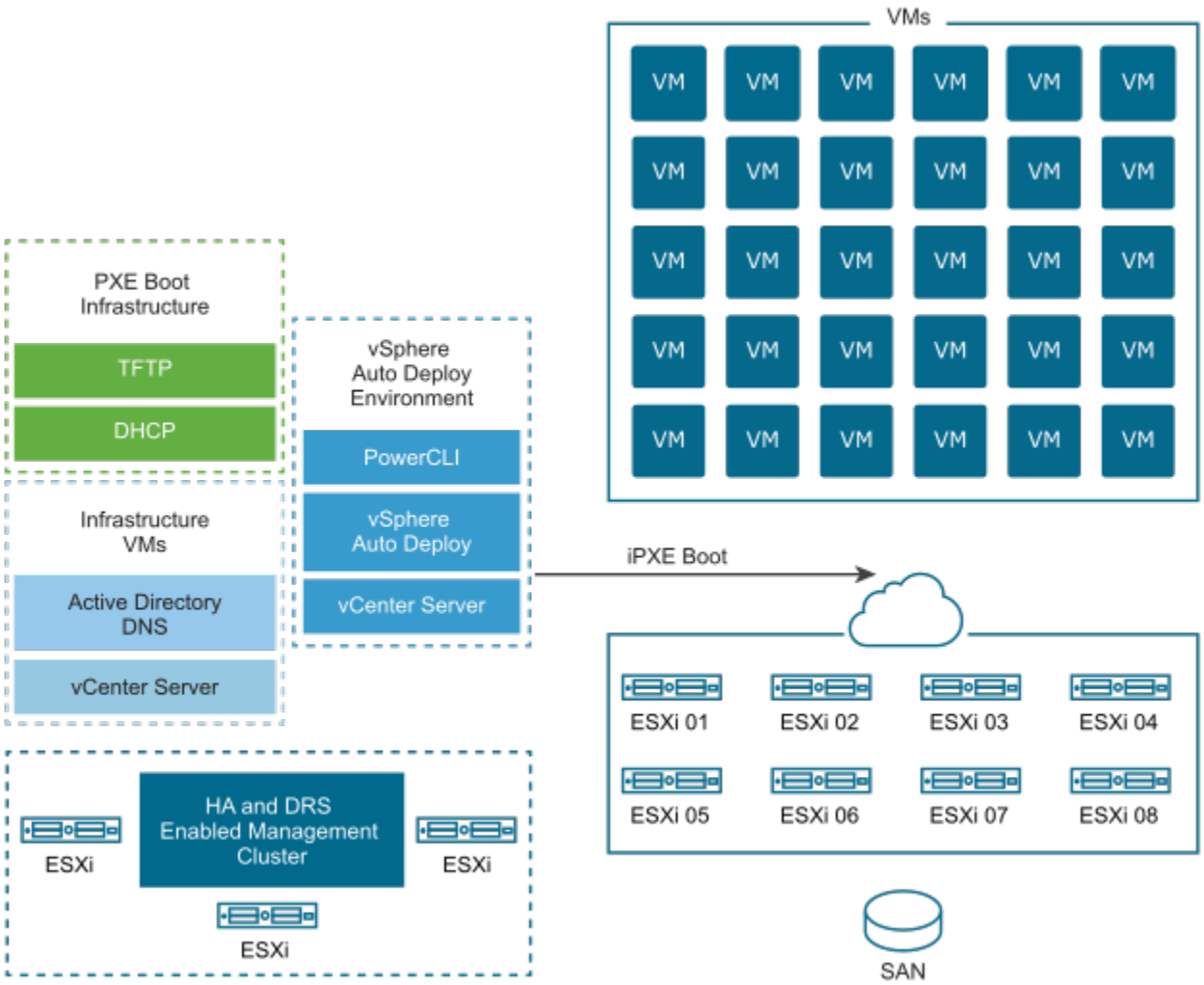
Set Up Highly Available vSphere Auto Deploy Infrastructure

In many production situations, a highly available vSphere Auto Deploy infrastructure is required to prevent data loss. Such infrastructure is also a prerequisite for using vSphere Auto Deploy with stateless caching.

For the management cluster, install ESXi on three hosts. Do not provision the management cluster hosts with vSphere Auto Deploy.

Watch the video "Highly Available vSphere Auto Deploy Infrastructure" for information about the implementation of a highly available vSphere Auto Deploy infrastructure:

Figure 10: Highly Available vSphere Auto Deploy Infrastructure



1. Enable vSphere HA and vSphere DRS on the management cluster.
2. Set up the following virtual machines on the management cluster.

Infrastructure Component	Description
PXE boot infrastructure	TFTP and DHCP servers.
Infrastructure VM	Active Directory, DNS, vCenter Server.
vSphere Auto Deploy environment	PowerCLI, vSphere Auto Deploy server, vCenter Server. Set up this environment on a single virtual machine or on three separate virtual machines in production systems.

   The vCenter Server on the infrastructure virtual machine differs from the vCenter Server in the vSphere Auto Deploy environment.
3. Set up vSphere Auto Deploy to provision other hosts as needed.

   Because the components on the management cluster are protected with vSphere HA, high availability is supported.

vSphere Auto Deploy Security Considerations

When you use vSphere Auto Deploy, mind networking security, boot image security, and potential password exposure to protect your environment.

Networking Security

Secure your network just as you secure the network for any other PXE-based deployment method. vSphere Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or of the Auto Deploy server is not checked during a PXE boot.

You can greatly reduce the security risk of Auto Deploy by completely isolating the network where Auto Deploy is used.

Boot Image and Host Profile Security

The boot image that the vSphere Auto Deploy server downloads to a machine can have the following components.

- The VIB packages that the image profile consists of are always included in the boot image.
- The host profile and host customization are included in the boot image if Auto Deploy rules are set up to provision the host with a host profile or host customization.
  - The administrator (root) password and user passwords that are included with host profile and host customization are hashed with SHA-512.
  - Any other passwords associated with profiles are in the clear. If you set up Active Directory by using host profiles, the passwords are not protected.

    Use the vSphere Authentication Proxy to avoid exposing the Active Directory passwords. If you set up Active Directory using host profiles, the passwords are not protected.
- The host's public and private SSL key and certificate are included in the boot image.

Device Alias Configuration

Device aliases, also called device names, are short names associated with I/O adapters in an I/O subsystem.

For example, network uplinks have aliases such as vmnic0, vmnic1, and so on. SCSI adapter objects in the storage subsystem and graphics device objects also have aliases. A hardware device can be presented as multiple I/O adapters in the I/O subsystem. The I/O adapters can be of a different type from the underlying physical device. For example, an FCoE device is a storage I/O adapter that uses NIC hardware. Software iSCSI is a storage adapter using the network stack at the IP layer. Therefore, in the ESXi native driver model, aliases formally refer only to I/O adapters, and not to physical devices such as a PCI NIC or a PCI HBA.

Device Alias Assignment

A stateless ESXi deployment model is one where the ESXi host is not installed on hard disks, and is typically booted by using PXE. A stateful ESXi deployment model is one where the ESXi host is installed on local hard disks. Device alias assignment occurs during a stateless ESXi boot or a fresh installation of stateful ESXi. The ESXi host assigns aliases to I/O adapters in an order which is based on the underlying hardware enumeration order. The ESXi host assigns aliases first to on-board devices and then to add-in cards based on slot order. The ESXi host cannot assign aliases to absent devices or devices without supported drivers.

An uplink that uses a NIC that is built into the motherboard receives a vmnicN alias with lower number compared to an uplink of a PCI add-in card. The NIC driver might register more than one uplink. If one of the uplinks does not correspond to an enumerable hardware device, the ESXi host assigns the next available alias to the uplink after the uplink is registered with the system.

Persistence of Device Alias Configuration

After the ESXi host assigns aliases, alias configuration is persisted. The ESXi host attempts to keep the alias of each device the same regardless of the ESXi version updates, or hardware changes, such as adding or removing devices from slots.

The persistence of the alias configuration depends on the deployment model.

- In stateful systems, the alias configuration is persisted locally on the host.
- In stateless systems, if you do not manage the stateless system by using host profiles, the alias configuration is not persisted locally on the host.
- In stateful and stateless systems that you manage by using host profiles, the alias configuration is persisted in the host profile. If you apply a host profile to a stateful host, the host profile overrides any locally persisted alias configuration.

Changes in the Device Alias Configuration

The persistence of alias configuration is based on the bus addresses of devices. If the bus address of a device is altered, the persisted alias configuration becomes inapplicable and the aliases assigned to the device might change.

Changes in the device alias configuration might occur in the following cases:

- A driver upgrade might enumerate or present an I/O adapter differently to the system compared to how the I/O adapter is presented before the driver upgrade.
- A stack upgrade might result in changes to parts of a multi-module driver setup, or to the ESXi I/O stack that supports a multi-module driver.
- BIOS or device firmware upgrades might lead to incomplete port or slot information.
- Changes in the slot position of a device.

Note: If you remove a device from the system, the alias configuration of the I/O adapters of the device is removed. If you add the same devices back to the system later, the I/O adapters of the device might not receive their previous aliases.

Device Alias Configuration in ESXi Clusters

Initial alias configuration is the same across a cluster of identical systems. However, even on a cluster that is considered homogenous, small differences in hardware or firmware might result in differences in the alias configuration between hosts.

Differences in the processing order during driver binding can also result in differences in alias configuration. For example, a NIC driver registers two uplinks, uplink-1 and uplink-2, for two ports of the same PCI device, where one of the ports is not hardware enumerable by the system. Timing changes in the order of registration of the uplinks might result in differences in how the ESXi hosts assign aliases to the uplinks. One ESXi host might assign the hardware-based alias to uplink-1, and another ESXi host might assign the hardware-based alias to uplink-2.

To match alias configuration across homogeneous hosts, you can use host profiles. The Device Alias Configuration host profile applies alias configuration to an ESXi host by mapping devices in the alias configuration to the ESXi host devices. The mapping operation is based on the hardware information sources that are used as the basis for initial alias assignment. For more information about information sources used for alias assignment, see the Knowledge Base article KB 2091560.

The Device Alias Configuration host profile also flags errors, for example, when a device is present in the host profile but not present on the host.

A heterogenous cluster does not have the same default alias configuration across its hosts. Due to the differences between the devices, a host profile cannot be applied cleanly.

Using ESXi Shell Commands to View Device Alias Information

On a running ESXi system, you can view information about I/O adapter aliases by running commands in an ESXi Shell.

Using ESXi Shell Commands to View Device Alias Information

Command	Description
`device alias list`	Lists all current I/O adapter aliases.
`device alias get -n<alias>`	Displays the physical device that an I/O adapter alias maps to.
`network nic list`	Lists aliases and general information about network devices.
`storage core adapter list`	Lists all storage I/O adapters.

Note: ESXCLI commands are supported commands. Using alternative sources for displaying alias information is not recommended.

Change Device Aliases on an ESXi Host by Using Host Profiles

You can modify a device alias on ESXi hosts by editing the device alias section of the host profile attached to the hosts.

A device alias change can occur, for example, when you apply a BIOS or device firmware update. For more information about changes in the device alias configuration, see Device Alias Configuration.

I/O adapters that are based on PCI hardware usually have a logical and a PCI alias entry. Both aliases must have the same value. Some I/O adapters usually have a logical alias entry only. PCI hardware devices without I/O adapters usually have a PCI alias entry only. Modify a PCI alias entry only when you need the alias for another device.

Note: Two different I/O adapters must not have the same alias, except I/O adapters that are based on PCI hardware and have a logical and a PCI alias entry.

Procedure

For information about exporting, extracting, and editing a host profile, see the *vSphere Host Profiles* documentation.

1. Export the current host profile attached to the ESXi host.
2. Extract a new host profile from the ESXi host, but do not apply the host profile.
3. Remove all entries from the device alias section of the current host profile.
4. Transfer all entries from the device alias section of the new host profile to the same section of the current host profile. You can modify the aliases in the entries before adding them to the current host profile.
5. Reapply the current host profile to the ESXi host.

Change Device Aliases on a Stateful ESXi Host by Using ESXCLI Commands

You can modify a device alias on a stateful ESXi host that does not have an attached host profile by running ESXCLI commands on the host.

A device alias change can occur, for example, when the slot position of a device changes. For more information about changes in the device alias configuration, see Device Alias Configuration.

Note: The following ESXCLI commands might not be compatible with ESXi version 6.7 and earlier.

1. To list the current assignment of aliases to device addresses, in the ESXi Shell, run `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias list`.

   For I/O adapters that are based on PCI hardware, you usually see a logical and a PCI alias entry.

   For some I/O adapters, you usually see a logical alias entry only.

   For PCI hardware devices without I/O adapters, you usually see a PCI alias entry only.

2. To change an alias, replace the `ALIAS`, `PCI_ADDRESS`, and `LOGICAL_ADDRESS` placeholder values with actual values, and follow one of the substeps.
   a) If an I/O adapter has a logical and a PCI alias, run `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type logical --alias ALIAS --bus-address LOGICAL_ADDRESS` and `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type pci --alias ALIAS --bus-address PCI_ADDRESS`.

      The logical and PCI aliases must have the same value.
   b) If an I/O adapter has a logical alias entry only, run `localcli --plugin-dir /usr/lib/vmware/esxcli/int/ deviceInternal alias store --bus-type logical --alias ALIAS --bus-address LOGICAL_ADDRESS`.
   c) If a PCI hardware device has a PCI alias entry only, run `localcli --plugin-dir /usr/lib/vmware/esxcli/ int/ deviceInternal alias store --bus-type pci --alias ALIAS --bus-address PCI_ADDRESS`.

      Modify a PCI alias only when you need the alias for another device.

   Note: Two different I/O adapters must not have the same alias, except I/O adapters that are based on PCI hardware and have a logical and a PCI alias entry.
3. Reboot the system.

Set Up vSphere Auto Deploy and Provision Hosts with vSphere PowerCLI

In this scenario, you are going to set up and configure a working vSphere Auto Deploy environment that includes four hosts. You will create rules and provision two of the hosts with an image profile and the other two with the same image profile and a host profile that is set up to prompt for user input.

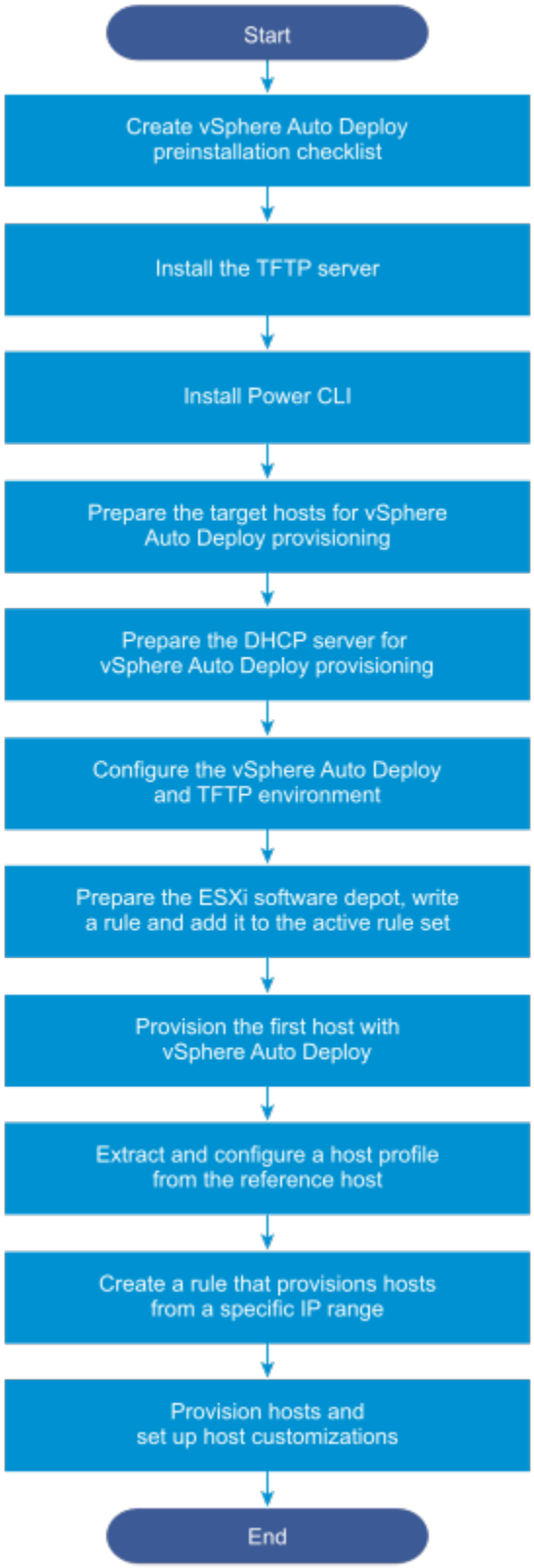
This scenario can provide you with the basis for a production environment. The task descriptions assume that you are using a flat network with no VLAN tagging between the physical hosts and the rest of your environment.

To perform the tasks in this scenario, you should have the following background knowledge and privileges.

- Experience with vSphere (vCenter Server and ESXi).
- Basic knowledge of Microsoft PowerShell and PowerCLI.
- Administrator rights to a Windows system and a vCenter Server system.

Follow the tasks in the order presented in this scenario. Some steps can be performed in a different order, but the order used here limits repeated manipulation of some components.

Figure 11: vSphere Auto Deploy Setup and Hosts Provisioning Workflow



vSphere Auto Deploy takes advantage of the iPXE infrastructure and PXE booting with legacy BIOS firmware is possible only over IPv4. If the hosts that you want to provision with vSphere Auto Deploy are with legacy BIOS, the vSphere Auto Deploy server must have an IPv4 address. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

vSphere Auto Deploy Preinstallation Checklist
Before you can start the tasks in this vSphere Auto Deploy scenario, make sure that your environment meets the hardware and software requirements, and that you have the necessary permissions for the components included in the setup.

Table 19: Preinstallation Checklist

Required Software and Hardware	Details
vCenter Server	The vSphere Auto Deploy server is part of vCenter Server. You must enable and start the vSphere Auto Deploy service on the vCenter Server system. You can perform many of the setup tasks by logging in to vCenter Server. See Prepare Your System for vSphere Auto Deploy.
Storage	Storage for ESXi datastores NFS, iSCSI, or Fibre Channel, with servers and storage arrays that are configured so the servers can detect the LUNs. • A list of target IP addresses for NFS or iSCSI. • A list of target volume information for NFS or iSCSI.
Host information (for four ESXi hosts)	A list of target IP addresses for NFS or iSCSI. A list of target volume information for NFS or iSCSI. • Default route, net mask, and primary and secondary DNS server IP addresses. • IP address and net mask for the VMkernel primary management network. • IP address and net mask for other VMkernel networks such as storage, vSphere FT, or VMware vMotion. vSphere Auto Deploy does not overwrite existing partitions by default.
PowerCLI	See Install PowerCLI.
ESXi software depot	The location of the ESXi software depot on the Downloads page of the VMware website. You use a URL to point to the image profile stored at that location, or you download a ZIP file to work with a local depot. Do not download the ESXi image.
TFTP server	TFTP installer software such as WinAgents TFTP server.
DHCP server	The DHCP server is included in the vSphere supported Windows Server versions.
DNS server	A working DNS server. You must add entries in both Forward (A Record) and Reverse (PTR Record) Zones for each target host.

You also need information about and administrator privileges to the core servers of the environment, including the ActiveDirectory server, DNS server, DHCP server, NTP server, and so on.

You must have complete control of the broadcast domain of the subnet in which you deploy the setup. Ensure that no other DHCP, DNS, or TFTP server are on this subnet.

Install the TFTP Server

To set up a vSphere Auto Deploy infrastructure, you must install a TFTP server in your environment. vSphere Auto Deploy relies on a TFTP server for sending a boot image to the hosts that it provisions.

This task only installs the TFTP server. You later download a configuration file to the server. See Configure the vSphere Auto Deploy and TFTP Environment in the vSphere Client.

1. Download your preferred TFTP server to a location that has network access to your vCenter Server and install the server.
2. Configure the TFTP root directory, for example `D:\TFTP_Root\`.

Install PowerCLI, to manage vSphere Auto Deploy with PowerCLI cmdlets.

Install PowerCLI

Before you can manage vSphere Auto Deploy with rules that you create with PowerCLI cmdlets, you must install PowerCLI.

Use the VMware PowerCLI User's Guide to learn about PowerShell basics, PowerCLI concepts, and how to install and configure PowerCLI.

Configure the settings of your target hosts to prepare them for provisioning with vSphere Auto Deploy.

Prepare the vSphere Auto Deploy Target Hosts

You must configure the BIOS settings of the four hosts and reconfirm the MAC address of the primary network device to prepare the target hosts for provisioning with vSphere Auto Deploy.

Hosts that you want to provision with vSphere Auto Deploy must meet the requirements for ESXi.

1. Change the BIOS settings of each of the four physical hosts to force the hosts to boot from the primary network device.
2. Reconfirm the MAC address of the primary network device.

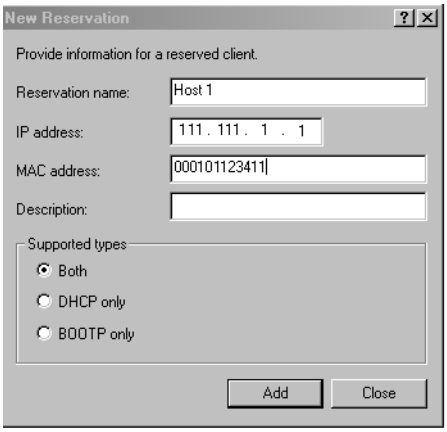
Set up the DHCP server to serve each target host with an iPXE binary.

Prepare the DHCP Server for vSphere Auto Deploy Provisioning

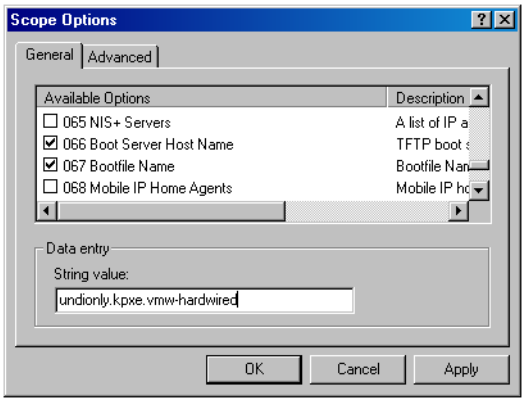
When you prepare the vSphere Auto Deploy target hosts, you must set up the DHCP server in this scenario to serve each target host with an iPXE binary.

The environment in this scenario uses Active Directory with DNS and DHCP. The DHCP server is included in the vSphere supported Windows Server versions.

1. Log in to your DHCP Server with administrator privileges.
2. Create a DHCP scope for your IP address range.
   a) Click **Start > Settings > Control Panel > Administrative Tools** and click **DHCP**.
   b) Navigate to **DHCP** > ***hostname*** > **IPv4**.
   c) Right-click **IPv4** and select **New Scope**.
   d) On the Welcome screen, click **Next**, and specify a name and description for the scope.
   e) Specify an IP address range and click **Next**.
   f) Click **Next** until you reach the Configure DHCP Options screen and select **No, I will configure this option later**.
3. Create a DHCP reservation for each target ESXi host.
   a) In the DHCP window, navigate to **DHCP** > ***hostname*** > **IPv4** > **Autodeploy Scope** > **Reservations**.
   b) Right-click **Reservations** and select **New Reservation**.
   c) In the New Reservation window, specify a name, IP address, and the MAC address for one of the hosts. Do not include the colon (:) in the MAC address.



   d) Repeat the process for each of the other hosts.
4. Set up the DHCP Server to point the hosts to the TFTP Server.
   a) In the DHCP window, navigate to **DHCP** > ***hostname*** > **IPv4** > **Autodeploy Scope** > **Scope Options**.
   b) Right click **Scope Options** and choose **Configure Options**.
   c) In the Scope Options window, click the **General** tab.
   d) Click **066 Boot Server Host Name** and enter the address of the TFTP server that you installed in the String value field below the Available Options.



e) Click **067 Bootfile Name** and enter `undionly.kpxe.vmw-hardwired`.

The `undionly.kpxe.vmw-hardwired` iPXE binary will be used to boot the ESXi hosts.

f) Click **Apply** and click **OK** to close the window.

5. In the DHCP window, right-click **DHCP** > ***hostname*** > **IPv4** > **Scope** > **Activate** and click **Activate**.
6. Do not log out from the DHCP Server if you are using Active Directory for DHCP and DNS, or log out otherwise.

start the vCenter Server service of vSphere Auto Deploy and configure the TFTP server.

Configure the vSphere Auto Deploy and TFTP Environment in the vSphere Client

After you prepare the DHCP server, you must start the vSphere Auto Deploy vCenter Server service and configure the TFTP server. You must download a TFTP ZIP file from your vSphere Auto Deploy server. The customized FTP server serves the boot images that vSphere Auto Deploy provides.

1. Use the vSphere Client to connect to the vCenter Server system that manages the vSphere Auto Deploy server.
2. Start the vSphere Auto Deploy service.
   a) Navigate to **Home** > **Auto Deploy**.
   b) On the **Auto Deploy** page, select your vCenter Server from the drop-down menu at the top.
   c) Click **Enable Auto Deploy and Image Builder** to activate the service.

   If the **Image Builder** service is already active, select the **Configure** tab and click **Enable Auto Deploy Service**.
3. In the Auto Deploy inventory, click the **Configure** tab.
4. Click the **Download TFTP Zip File**.
5. Save the file `deploy-tftp.zip` to the `TFTP_Root` directory that you created when you installed the TFTP Server, and unzip the file.

Add a software depot to your inventory and use an image profile from the depot to create a rule for host provisioning.

Prepare the ESXi Software Depot and Write a Rule

After you configure the vSphere Auto Deploy infrastructure, you must add an ESXi software depot, specify an image profile, write a rule, and add it to the active rule set.

Verify that you can access the ESXi hosts that you want to provision from the system on which you run PowerCLI.

vSphere Auto Deploy provisions hosts with image profiles that define the set of VIBs that an ESXi installation process uses. Image profiles are stored in software depots. You must make sure that the correct image profile is available before you start provisioning hosts. When you add a software depot to a PowerCLI session, it is available only during the current session. It does not persist across sessions.

The steps in this task instruct you to run PowerCLI cmdlets. For additional information about the vSphere Auto Deploy cmdlets that you can run in a PowerCLI session, see vSphere Auto Deploy PowerCLI Cmdlet Overview.

1. Log in as an administrator to the console of the Windows system, either directly or by using RDP.

   This task assumes that you installed PowerCLI on the system on which the vCenter Server system is running.

2. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate issues occur. In a development environment, you can ignore the warning.

3. Enter the vCenter Server credentials.

4. Run `Add-EsxSoftwareDepot` to add the online depot to the PowerCLI session.

   ```
   Add-EsxSoftwareDepot https://dl.broadcom.com/<Download Token>/PROD/COMP/ESX_HOST/main/vmw-depot-index.xml
   ```

   Adding the software depot is required each time you start a new PowerCLI session.

   Note:

   The URLs of the official VMware online depot are now unique for each customer. To update the download sources URLs, see the following KB articles: 390121 and 390123.

5. Validate that you successfully added the software depot by checking the contents of the depot with the `Get-EsxImageProfile` cmdlet.

   The cmdlet returns information about all image profiles in the depot.

6. Create a new rule by running the `New-DeployRule` cmdlet.

   ```
   New-DeployRule -Name "InitialBootRule" -Item ESXi-6.0.0-2494585-standard -AllHosts
   ```

   The cmdlet creates a rule that assigns the specified image profile to all hosts in the inventory.

7. Add the new rule to the active rule set to make the rule available to the vSphere Auto Deploy server.

   ```
   Add-DeployRule -DeployRule "InitialBootRule"
   ```

Provision your first host with vSphere Auto Deploy and verify its image provisioning.

Provision the First Host with vSphere Auto Deploy

After creating a rule and adding it to the active rule set, you can provision the first host and check its vCenter Server location to complete verification of the image provisioning of your setup.

1. Open a console session to the physical host that you want to use as the first ESXi target host, boot the host, and look for messages that indicate a successful iPXE boot.

   During the boot process, DHCP assigns an IP address to the host. The IP address matches the name you specified earlier in the DNS server. The host contacts the vSphere Auto Deploy server and downloads the ESXi binaries from the HTTP URL indicated in the iPXE tramp file that you downloaded earlier to the TFTP_Root directory. Each instance of vSphere Auto Deploy produces a custom set of files for the TFTP Server.

2. Use the vSphere Client to connect to the vCenter Server system that manages the vSphere Auto Deploy server.

3. On the vSphere Client Home page, click **Hosts and Clusters**.

4. Verify that the newly provisioned host is now in the vCenter Server inventory at the datacenter level.

   By default, vSphere Auto Deploy adds hosts at the datacenter level when the boot process completes.

Extract a host profile from the host and configure it to require user input.

Extract and Configure a Host Profile from the Reference Host
After provisioning the first host, you can extract and configure a host profile that can be used to apply the same configuration to other target hosts. Configuration that differs for different hosts, such as a static IP address, can be managed through the host customization mechanism.

vSphere Auto Deploy can provision each host with the same host profile. vSphere Auto Deploy can also use host customization that allows you to specify different information for different hosts. For example, if you set up a VMkernel port for vMotion or for storage, you can specify a static IP address for the port by using the host customization mechanism.

1. Use the vSphere Client to connect to the vCenter Server system that manages the vSphere Auto Deploy server.
2. Click **Policies and Profiles** and select **Host Profiles**.
3. Click **Extract Host Profile**.
4. On the **Select host** page of the wizard, select the reference host that you configured earlier and click **Next**.
5. On the **Name and Description** page of the wizard, enter a name and description for the new profile and click **Finish**.
6. Select the host profile that you want to edit and click the **Configure** tab.
7. Click **Edit Host Profile**.
8. Select **Security and Services** > **Security Settings** > **Security** > **User Configuration** > **root**.
9. From the **Password** drop-down menu, select **User Input Password Configuration**.
10. Click **Save** to configure the host profile settings.

Create a vSphere Auto Deploy rule to apply the host profile to other ESXi hosts.

Create a Rule that Provisions Hosts from a Specific IP Range
After creating a host profile from a reference host, you can create a rule that applies the previously verified image profile and the host profile that you extracted to target hosts from a specific IP range.

1. Log in with administrator privileges to the console of the Windows system, either directly or by using RDP.
2. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate issues occur. In a development environment, you can ignore the warning.
3. Run `Add-EsxSoftwareDepot` to add the online depot to the PowerCLI session.

   ```
   Add-EsxSoftwareDepot https://dl.broadcom.com/<Download Token>/PROD/COMP/ESX_HOST/main/vmw-depot-index.xml
   ```

   Adding the software depot is required each time you start a new PowerCLI session.

   Note:

   The URLs of the official VMware online depot are now unique for each customer. To update the download sources URLs, see the following KB articles: 390121 and 390123.
4. Required: Display the rules in the active rule set by running the `Get-DeployRuleset` cmdlet.
5. Create a rule that instructs vSphere Auto Deploy to provision the set of hosts from a specified IP range with the image profile that you previously selected and the host profile that you created from the reference host.

   ```
   New-DeployRule -name "Production01Rule" -item "image_profile",ESXGold -Pattern "ipv4=IP_range"
   ```
6. Add the new rule to the active rule set.

   ```
   Add-DeployRule -DeployRule "Production01Rule"
   ```

7. Check the active rule set by running the `Get-DeployRuleset` command.
   PowerCLI displays information similar to the following example.

```
Name:              Production01Rule
PatternList:       {ipv4=address_range}
ItemList:          {ESX-version-XXXXXX-standard, Compute01, ESXGold}
```

Provision the hosts and set up the host customizations.

Provision Hosts and Set Up Host Customizations
With the rule in place that provisions hosts using an image profile and a host profile, you can provision specific target hosts. If any host profile items are set to prompt the user for input, the host comes up in maintenance mode. You apply the host profile or check host compliance to be prompted for the information. The system associates the host customization with the host.

1. Boot the remaining hosts you want to provision.
   vSphere Auto Deploy boots the hosts, applies the host profile, and adds the hosts to the vCenter Server inventory. The hosts remain in maintenance mode because the host profile from the reference host is set up to require user input for each host.
2. Use the vSphere Client to connect to the vCenter Server system that manages the vSphere Auto Deploy server.
3. Click **Policies and Profiles** and select **Host Profiles**.
4. Right-click the newly created host profile for Auto Deploy and click **Edit Host Customizations**.
5. Select the hosts, enter the required host customizations and click **Finish**.
   Alternatively, you can also **Import Host Customizations** file.
6. Apply the host profile to each of the hosts and get the hosts out of maintenance mode. Alternatively, you can reboot each host.
   When the reboot progress completes, all hosts are running with the image you specify and use the configuration in the reference host profile. The cluster shows that all hosts are fully compliant.

All hosts are now configured with the shared information through the reference host profile and with the host-specific information through the host customization mechanism. The next time you boot the hosts, they receive the complete Host Profile information, including the host-specific information, and boot up completely configured and out of Maintenance Mode.

Troubleshooting vSphere Auto Deploy

The vSphere Auto Deploy troubleshooting topics cover some situations when provisioning hosts with vSphere Auto Deploy does not work as expected.

- vSphere Auto Deploy TFTP Timeout Error at Boot Time
- vSphere Auto Deploy Host Boots with Wrong Configuration
- Host Is Not Redirected to vSphere Auto Deploy Server
- Package Warning Message When You Assign an Image Profile to a vSphere Auto Deploy Host
- vSphere Auto Deploy Host with a Built-In USB Flash Drive Does Not Send Coredumps to Local Disk
- vSphere Auto Deploy Host Reboots After Five Minutes
- vSphere Auto Deploy Host Cannot Contact TFTP Server
- vSphere Auto Deploy Host Cannot Retrieve ESXi Image from vSphere Auto Deploy Server
- vSphere Auto Deploy Host Does Not Get a DHCP Assigned Address
- vSphere Auto Deploy Host Does Not Network Boot
- Recovering from Database Corruption on the vSphere Auto Deploy Server

vSphere Auto Deploy TFTP Timeout Error at Boot Time

A TFTP Timeout error message appears when a host provisioned with vSphere Auto Deploy boots. The text of the message depends on the BIOS.

A TFTP Timeout error message appears when a host provisioned with vSphere Auto Deploy boots. The text of the message depends on the BIOS.

The TFTP server is down or unreachable.

- Ensure that your TFTP service is running and reachable by the host that you are trying to boot.
- To view the diagnostic logs for details on the present error, see your TFTP service documentation.

vSphere Auto Deploy Host Boots with Wrong Configuration

A host is booting with a different ESXi image, host profile, or folder location than the one specified in the rules.

A host is booting with a different ESXi image profile or configuration than the image profile or configuration that the rules specify. For example, you change the rules to assign a different image profile, but the host still uses the old image profile.

After the host has been added to a vCenter Server system, the boot configuration is determined by the vCenter Server system. The vCenter Server system associates an image profile, host profile, or folder location with the host.

Use the `Test-DeployRuleSetCompliance` and `Repair-DeployRuleSetCompliance` vSphere PowerCLI cmdlets to reevalute the rules and to associate the correct image profile, host profile, or folder location with the host.

Host Is Not Redirected to vSphere Auto Deploy Server

During boot, a host that you want to provision with vSphere Auto Deploy loads iPXE. The host is not redirected to the vSphere Auto Deploy server.

During boot, a host that you want to provision with vSphere Auto Deploy loads iPXE. The host is not redirected to the vSphere Auto Deploy server.

The `tramp` file that is included in the TFTP ZIP file has the wrong IP address for the vSphere Auto Deploy server.

Correct the IP address of the vSphere Auto Deploy server in the `tramp` file, as explained in the *vSphere Installation and Setup* documentation.

Package Warning Message When You Assign an Image Profile to a vSphere Auto Deploy Host

When you run a vSphere PowerCLI cmdlet that assigns an image profile that is not vSphere Auto Deploy ready, a warning message appears.

When you write or modify rules to assign an image profile to one or more hosts, the following error results:

```
Warning: Image Profile <name-here> contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy.
```

Each VIB in an image profile has a `stateless-ready` flag that indicates that the VIB is meant for use with vSphere Auto Deploy. You get the error if you attempt to write a vSphere Auto Deploy rule that uses an image profile in which one or more VIBs have that flag set to FALSE.

Note: You can use hosts provisioned with vSphere Auto Deploy that include VIBs that are not stateless ready without problems. However booting with an image profile that includes VIBs that are not stateless ready is treated like a fresh

install. Each time you boot the host, you lose any configuration data that would otherwise be available across reboots for hosts provisioned with vSphere Auto Deploy.

1. Use vSphere ESXi Image Builder cmdlets in a vSphere PowerCLI session to view the VIBs in the image profile.
2. Remove any VIBs that are not stateless-ready.
3. Rerun the vSphere Auto Deploy cmdlet.

vSphere Auto Deploy Host with a Built-In USB Flash Drive Does Not Send Coredumps to Local Disk

If your vSphere Auto Deploy host has a built-in USB flash drive, and an error results in a coredump, the coredump is lost. Set up your system to use ESXi Dump Collector to store coredumps on a networked host.

If your vSphere Auto Deploy host has a built-in USB Flash, and if it encounters an error that results in a coredump, the coredump is not sent to the local disk.

1. Install ESXi Dump Collector on a system of your choice.
   ESXi Dump Collector is included with the vCenter Server installer.
2. Use ESXCLI to configure the host to use ESXi Dump Collector.

   ```
   esxcli conn_options system coredump network set IP-addr,port
   esxcli system coredump network set -e true
   ```

3. Use ESXCLI to deactivate local coredump partitions.

   ```
   esxcli conn_options system coredump partition set -e false
   ```

vSphere Auto Deploy Host Reboots After Five Minutes

A vSphere Auto Deploy host boots and displays iPXE information, but reboots after five minutes.

A host to be provisioned with vSphere Auto Deploy boots from iPXE and displays iPXE information on the console. However, after five minutes, the host displays the following message to the console and reboots.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

The host might also display the following details:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

The console then displays the host's machine attributes including vendor, serial number, IP address, and so on.

No image profile is currently associated with this host.

You can assign an image profile to the host by running the `Apply-EsxImageProfile` cmdlet, or by creating the following rule:

1. Run the `New-DeployRule` cmdlet to create a rule that includes a pattern that matches the host with an image profile.
2. Run the `Add-DeployRule` cmdlet to add the rule to a ruleset.

3. Run the `Test-DeployRuleSetCompliance` cmdlet and use the output of that cmdlet as the input to the `Repair-DeployRuleSetCompliance` cmdlet.

vSphere Auto Deploy Host Cannot Contact TFTP Server

The host that you provision with vSphere Auto Deploy cannot contact the TFTP server.

When you attempt to boot a host provisioned with vSphere Auto Deploy, the host performs a network boot and is assigned a DHCP address by the DHCP server, but the host cannot contact the TFTP server.

The TFTP server might have stopped running, or a firewall might block the TFTP port.

- If you installed the WinAgents TFTP server, open the WinAgents TFTP management console and verify that the service is running. If the service is running, check the Windows firewall's inbound rules to make sure the TFTP port is not blocked. Turn off the firewall temporarily to see whether the firewall is the problem.
- For all other TFTP servers, see the server documentation for debugging procedures.

vSphere Auto Deploy Host Cannot Retrieve ESXi Image from vSphere Auto Deploy Server

The host that you provision with vSphere Auto Deploy stops at the iPXE boot screen.

When you attempt to boot a host provisioned with vSphere Auto Deploy, the boot process stops at the iPXE boot screen and the status message indicates that the host is attempting to get the ESXi image from the vSphere Auto Deploy server.

The vSphere Auto Deploy service might be stopped or the vSphere Auto Deploy server might be unaccessible.

1. Log in to the system on which you installed the vSphere Auto Deploy server.
2. Check that the vSphere Auto Deploy server is running.
   a) Click **Start** > **Settings** > **Control Panel** > **Administrative Tools**.
   b) Double-click **Services** to open the Services Management panel.
   c) In the Services field, look for the VMware vSphere Auto Deploy Waiter service and restart the service if it is not running.
3. Open a Web browser, enter the following URL, and check whether the vSphere Auto Deploy server is accessible.

   https://*Auto_Deploy_Server_IP_Address*:*Auto_Deploy_Server_Port*/vmw/rdb

   Note: Use this address only to check whether the server is accessible.
4. If the server is not accessible, a firewall problem is likely.
   a) Try setting up permissive TCP Inbound rules for the vSphere Auto Deploy server port.

      The port is 6501 unless you specified a different port during installation.
   b) As a last resort, deactivate the firewall temporarily and enable it again after you verified whether it blocked the traffic. Do not deactivate the firewall on production environments.

      To deactivate the firewall, run `netsh firewall set opmode disable`. To enable the firewall, run `netsh firewall set opmode enable`.

vSphere Auto Deploy Host Does Not Get a DHCP Assigned Address

The host you provision with vSphere Auto Deploy fails to get a DHCP Address.

When you attempt to boot a host provisioned with vSphere Auto Deploy, the host performs a network boot but is not assigned a DHCP address. The vSphere Auto Deploy server cannot provision the host with the image profile.

You might have a problem with the DHCP service or with the firewall setup.

1. Check that the DHCP server service is running on the Windows system on which the DHCP server is set up to provision hosts.
   a) Click **Start** > **Settings** > **Control Panel** > **Administrative Tools**.
   b) Double-click **Services** to open the Services Management panel.
   c) In the Services field, look for the DHCP server service and restart the service if it is not running.
2. If the DHCP server is running, recheck the DHCP scope and the DHCP reservations that you configured for your target hosts.

   If the DHCP scope and reservations are configured correctly, the problem most likely involves the firewall.
3. As a temporary workaround, turn off the firewall to see whether that resolves the problem.
   a) Open the command prompt by clicking **Start** > **Program** > **Accessories** > **Command prompt**.
   b) Type the following command to temporarily turn off the firewall. Do not turn off the firewall in a production environment.

      ```
      netsh firewall set opmode disable
      ```
   c) Attempt to provision the host with vSphere Auto Deploy.
   d) Type the following command to turn the firewall back on.

      ```
      netsh firewall set opmode enable
      ```
4. Set up rules to allow DHCP network traffic to the target hosts.

   See the firewall documentation for DHCP and for the Windows system on which the DHCP server is running for details.

vSphere Auto Deploy Host Does Not Network Boot

The host you provision with vSphere Auto Deploy comes up but does not network boot.

When you attempt to boot a host provisioned with vSphere Auto Deploy, the host does not start the network boot process.

You did not enable your host for network boot.

1. Reboot the host and follow the on-screen instructions to access the BIOS configuration.
2. In the BIOS configuration, enable Network Boot in the Boot Device configuration.

Recovering from Database Corruption on the vSphere Auto Deploy Server

In some situations, you might have a problem with the vSphere Auto Deploy database. The most efficient recovery option is to replace the existing database file with the most recent backup.

When you use vSphere Auto Deploy to provision the ESXi hosts in your environment, you might encounter a problem with the vSphere Auto Deploy database.

Important: This is a rare problem. Follow all other vSphere Auto Deploy troubleshooting strategies before you replace the current database file. Rules or associations that you created since the backup you choose are lost.

This problem happens only with hosts that are provisioned with vSphere Auto Deploy.

1. Stop the vSphere Auto Deploy server service.
2. Find the vSphere Auto Deploy log by going to the vSphere Auto Deploy page in the vSphere Client.
3. Check the logs for the following message:

   ```
   DatabaseError: database disk image is malformed.
   ```

   If you see the message, replace the existing database with the most recent backup.

4. Go to the vSphere Auto Deploy data directory at `/var/lib/rbd`.
   The directory contains a file named `db`, and backup files named `db-yyy-mm-dd`.
5. Rename the current `db` file.
   VMware Support might ask for that file if you call for assistance.
6. Rename the most recent backup to `db`.
7. Restart the vSphere Auto Deploy server service.
8. If the message still appears in the log, repeat the steps to use the next recent backup until vSphere Auto Deploy works without database errors.

Setting Up ESXi

These topics provide information about using the direct console user interface and configuring defaults for ESXi.

- ESXi Autoconfiguration
- About the Direct Console ESXi Interface
- Enable ESXi Shell and SSH Access with the Direct Console User Interface
- Managing ESXi Remotely
- Set the Password for the Administrator Account
- Configuring the BIOS Boot Settings
- Configuring Network Settings
- Storage Behavior
- Configuring System Logging
- Set the Host Image Profile Acceptance Level
- Remove All Custom Packages on ESXi
- Modify ESXi Configuration Files
- Deactivate Support for Non-ASCII Characters on ESXi
- Reset the System Configuration

ESXi Autoconfiguration

When you turn on the ESXi host for the first time or after resetting the configuration defaults, the host enters an autoconfiguration phase. This phase configures system network and storage devices with default settings.

By default, Dynamic Host Configuration Protocol (DHCP) configures IP, and all visible blank internal disks are formatted with the virtual machine file system (VMFS) so that virtual machines can be stored on the disks.

About the Direct Console ESXi Interface

Use the direct console interface for initial ESXi configuration and troubleshooting.

Connect a keyboard and monitor to the host to use the direct console. After the host completes the autoconfiguration phase, the direct console appears on the monitor. You can examine the default network configuration and change any settings that are not compatible with your network environment.

Key operations available to you in the direct console include:

- Configuring hosts
- Setting up administrative access
- Troubleshooting

You can also use vSphere Client to manage the host by using vCenter Server.

Table 20: Navigating in the Direct Console

Action	Key
View and change the configuration	F2
Change the user interface to high-contrast mode	F4
Shut down or restart the host	F12
View the VMkernel log	Alt+F12
Switch to the shell console	Alt+F1
Switch to the direct console user interface	Alt+F2
Move the selection between fields	Arrow keys
Select a menu item	Enter
Toggle a value	Spacebar
Confirm sensitive commands, such as resetting configuration defaults	F11
Save and exit	Enter
Exit without saving	Esc
Exit system logs	q

Configure the Keyboard Layout for the Direct Console

You can configure the layout for the keyboard that you use with the direct console.

1. From the direct console, select **Configure Keyboard** and press Enter.
2. Select the layout to use.
3. Press the spacebar to toggle selections on and off.
4. Press Enter.

Create a Security Banner for the Direct Console

A security banner is a message that is displayed on the direct console **Welcome** screen.

1. From the vSphere Client, connect to the vCenter Server.
2. Select the host in the inventory.
3. Click the **Configure** tab.
4. Under System, select **Advanced System Settings**.
5. Select `Annotations.WelcomeMessage`.
6. Click the **Edit** icon.
7. Enter a security message.

The message is displayed on the direct console **Welcome** screen.

Redirecting the Direct Console to a Serial Port

To manage your ESXi host remotely from a serial console, you can redirect the direct console to a serial port.

vSphere supports the VT100 terminal type and the PuTTy terminal emulator to view the direct console over the serial port.

You can redirect the direct console to a serial port in several ways.

Redirect the Direct Console to a Serial Port by Setting the Boot Options Manually

When you redirect the direct console to a serial port by setting the boot options, the change does not persist for subsequent boots.

Verify that the serial port is not in use for serial logging and debugging.

1. Start the host.
2. When the Loading VMware Hypervisor window appears, press Shift+O to edit boot options.
3. Deactivate the logPort and gdbPort on com1 and set tty2Port to com1 by entering the following boot options:

   ```
   "gdbPort=none logPort=none tty2Port=com1";
   ```

   To use com2 instead, replace `com1` with `com2` .

The direct console is redirected to the serial port until you reboot the host. To redirect the direct console for subsequent boots, see Redirect the Direct Console to a Serial Port from the vSphere Client

Related Links

Redirect the Direct Console to a Serial Port from the vSphere Client on page 1132

You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy on page 1133

After you redirect the direct console to a serial port, you can make that setting part of the host profile that persists when you reprovision the host with Auto Deploy.

Redirect the Direct Console to a Serial Port from the vSphere Client

You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

- Verify that you can access the host from the vSphere Client.
- Verify that the serial port is not in use for serial logging and debugging, or for ESX Shell (tty1Port).

1. From the vSphere Client, connect to the vCenter Server.
2. Select the host in the inventory.
3. Click the **Configure** tab.
4. Under System, select **Advanced System Settings**.
5. Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.
6. Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: `com1` or `com2`.
7. Reboot the host.

You can now manage the ESXi host remotely from a console that is connected to the serial port.

Related Links

Redirect the Direct Console to a Serial Port by Setting the Boot Options Manually on page 1132

When you redirect the direct console to a serial port by setting the boot options, the change does not persist for subsequent boots.

Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy on page 1133
After you redirect the direct console to a serial port, you can make that setting part of the host profile that persists when you reprovision the host with Auto Deploy.

Redirect the Direct Console to a Serial Port in a Host Deployed with Auto Deploy

After you redirect the direct console to a serial port, you can make that setting part of the host profile that persists when you reprovision the host with Auto Deploy.

The serial port must not already be in use for serial logging and debugging.

1. From the , connect to the vCenter Server.
2. Select the host in the inventory.
3. Under System, select **Advanced System Settings**.
4. Make sure that the **VMkernel.Boot.logPort** and **VMkernel.Boot.gdbPort** fields are not set to use the com port that you want to redirect the direct console to.
5. Set **VMkernel.Boot.tty2Port** to the serial port to redirect the direct console to: `com1` or `com2`.
6. Click **OK**.
7. Save the host profile and attach the host to the profile. See the *vSphere Host Profiles* documentation.

The setting to redirect the direct console to a serial port is stored by vCenter Server and persists when you reprovision the host with Auto Deploy.

Related Links

Redirect the Direct Console to a Serial Port by Setting the Boot Options Manually on page 1132
When you redirect the direct console to a serial port by setting the boot options, the change does not persist for subsequent boots.

Redirect the Direct Console to a Serial Port from the vSphere Client on page 1132
You can manage the ESXi host remotely from a console that is connected to the serial port by redirecting the direct console to either of the serial ports com1 or com2. When you use the vSphere Client to redirect the direct console to a serial port, the boot option that you set persists after subsequent reboots.

Enable ESXi Shell and SSH Access with the Direct Console User Interface

Use the direct console user interface to enable the ESXi Shell.

1. From the Direct Console User Interface, press F2 to access the System Customization menu.
2. Select **Troubleshooting Options** and press Enter.
3. From the Troubleshooting Mode Options menu, select a service to enable.
   - Enable ESXi Shell
   - Enable SSH

4. Press Enter to enable the service.
5. Optional: Set the timeout for the ESXi Shell.

   By default, timeouts for the ESXi Shell is 0 (not active).

   The availability timeout setting is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, if you have not logged in, the shell is deactivated.

   Note: If you are logged in when the timeout period elapses, your session will persist. However, the ESXi Shell is deactivated, preventing other users from logging in.

   a) From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.
   b) Enter the availability timeout in minutes.

      The availability timeout is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled.
   c) Press Enter.
   d) Enter the idle timeout.

      The idle timeout is the number of minutes that can elapse before the user is logged out of an idle interactive sessions. Changes to the idle timeout apply the next time a user logs in to the ESXi Shell and do not affect existing sessions.
6. Press Esc until you return to the main menu of the Direct Console User Interface.

Managing ESXi Remotely

You can use the VMware Host Client, the vSphere Client and vCenter Server to manage your ESXi hosts.

For instructions about downloading and installing vCenter Server and the vCenter Server components, see *vCenter Server Installation and Setup*. For information about installing the VMware Host Client, see *vSphere Single Host Management*.

Set the Password for the Administrator Account

You can use the direct console to set the password for the administrator account (root).

The administrative user name for the ESXi host is root. By default, the administrative password is not set.

1. From the direct console, select **Configure Password**.
2. Optional: If a password is already set up, type the password in the **Old Password** line and press Enter.
3. In the **New Password** line, type a new password and press Enter.
4. Retype the new password and press Enter.

Configuring the BIOS Boot Settings

If your server has multiple drives, you might need to configure the BIOS settings.

The BIOS boot configuration determines how your server boots. Generally, the CD-ROM device is listed first.

Note: If you are using ESXi Embedded, the BIOS boot configuration determines whether your server boots into the ESXi boot device or another boot device. Generally, the USB flash device is listed first in the BIOS boot settings on the machine that hosts ESXi.

You can change the boot setting by configuring the boot order in the BIOS during startup or by selecting a boot device from the boot device selection menu. When you change the boot order in the BIOS, the new setting affects all subsequent reboots. When you select a boot device from the boot device selection menu, the selection affects the current boot only.

Some servers do not have a boot device selection menu, in which case you must change the boot order in the BIOS even for one-time boots, and then change it back again during a subsequent reboot.

Change the BIOS Boot Setting for ESXi

Configure the BIOS boot setting for ESXi if you want the server to boot into ESXi by default.

ESXi Installable and ESXi Embedded cannot exist on the same host.

1. While the ESXi host is powering on, press the key required to enter your host's BIOS setup.
   Depending on your server hardware, the key might be a function key or Delete. The option to enter the BIOS setup might be different for your server.
2. Select the BIOS boot setting.

Option	Description
If you are using the installable version of ESXi	Select the disk on which you installed the ESXi software and move it to the first position in the list. The host boots into ESXi.
If you are using ESXi Embedded	Select the USB flash device and move it to the first position in the list. The host starts in ESXi mode.

Configure the Boot Setting for Virtual Media

If you are using remote management software to set up ESXi, you might need to configure the boot setting for virtual media.

ESXi Installable and ESXi Embedded cannot exist on the same host.

Virtual media is a method of connecting a remote storage media such as CD-ROM, USB mass storage, ISO image, and floppy disk to a target server that can be anywhere on the network. The target server has access to the remote media, and can read from and write to it as if it were physically connected to the server's USB port.

1. Connect the media to the virtual device.
   For example, if you are using a Dell server, log in to the Dell Remote Access Controller (DRAC) or a similar remote management interface and select a physical floppy or CD-ROM drive, or provide a path to a floppy image or CD-ROM image.
2. Reboot the server.
3. While the server is powering on, enter the device selection menu.
   Depending on your server hardware, the key might be a function key or Delete.
4. Follow the instructions to select the virtual device.

The server boots from the configured device once and goes back to the default boot order for subsequent boots.

Configuring Network Settings

ESXi requires one IP address for the management network. To configure basic network settings, use the vSphere Client or the direct console.

Use the vSphere Client if you are satisfied with the IP address assigned by the DHCP server.

Use the direct console for network configuration in the following cases:

- You are not satisfied with the IP address assigned by the DHCP server.
- You are not allowed to use the IP address assigned by the DHCP server.
- ESXi does not have an IP address. This situation might occur if the autoconfiguration phase did not succeed in configuring DHCP.

- The wrong network adapter was selected during the autoconfiguration phase.

Use ESXCLI commands to configure your network settings. See esxcli network Commands.

Network Access to Your ESXi Host

The default behavior is to configure the ESXi management network using DHCP. You can override the default behavior and use static IP settings for the management network after the installation is completed.

Table 21: Network Configuration Scenarios Supported by ESXi

Scenario	Approach
You want to accept the DHCP-configured IP settings.	In the ESXi direct console, you can find the IP address assigned through DHCP to the ESXi management interface. You can use that IP address to connect to the host from the vSphere Client and customize settings, including changing the management IP address.
One of the following is true: • You do not have a DHCP server. • The ESXi host is not connected to a DHCP server. • Your connected DHCP server is not functioning properly.	During the autoconfiguration phase, the software assigns the link local IP address, which is in the subnet 169.254.x.x/16. The assigned IP address appears on the direct console. You can override the link local IP address by configuring a static IP address using the direct console.
The ESXi host is connected to a functioning DHCP server, but you do not want to use the DHCP-configured IP address.	During the autoconfiguration phase, the software assigns a DHCP-configured IP address. You can make the initial connection by using the DHCP-configured IP address. Then you can configure a static IP address. If you have physical access to the ESXi host, you can override the DHCP-configured IP address by configuring a static IP address using the direct console.
Your security deployment policies do not permit unconfigured hosts to be powered on the network.	Follow the setup procedure in Configure the Network Settings on a Host That Is Not Attached to the Network.

ESXi Networking Security Recommendations

Isolation of network traffic is essential to a secure ESXi environment. Different networks require a different access and level of isolation.

Your ESXi host uses several networks. Use appropriate security measures for each network, and isolate traffic for specific applications and functions. For example, ensure that VMware vSphere® vMotion® traffic does not travel over networks where virtual machines are located. Isolation prevents snooping. Having separate networks is also recommended for performance reasons.

- vSphere infrastructure networks are used for features such as vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN, and storage. Isolate these networks for their specific functions. It is often not necessary to route these networks outside a single physical server rack.
- A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from other traffic. This network should be accessible only by system, network, and security administrators. Use jump box or virtual private network (VPN) to secure access to the management network. Strictly control access within this network.
- Virtual machine traffic can flow over one or many networks. You can enhance the isolation of virtual machines by using virtual firewall solutions that set firewall rules at the virtual network controller. These settings travel with a virtual machine as it migrates from host to host within your vSphere environment.

Choose Network Adapters for the Management Network

Traffic between an ESXi host and any external management software is transmitted through an Ethernet network adapter on the host. You can use the direct console to choose the network adapters that are used by the management network.

Examples of external management software include the vCenter Server and SNMP client. Network adapters on the host are named vmnic*N*, where N is a unique number identifying the network adapter, for example, vmnic0, vmnic1, and so forth.

During the autoconfiguration phase, the ESXi host chooses vmnic0 for management traffic. You can override the default choice by manually choosing the network adapter that carries management traffic for the host. In some cases, you might want to use a Gigabit Ethernet network adapter for your management traffic. Another way to help ensure availability is to select multiple network adapters. Using multiple network adapters enables load balancing and failover capabilities.

1. From the direct console, select **Configure Management Network** and press Enter.
2. Select **Network Adapters** and press Enter.
3. Select a network adapter and press Enter.

After the network is functional, you can use the vSphere Client to connect to the ESXi host through vCenter Server.

Set the VLAN ID

You can set the virtual LAN (VLAN) ID number of the ESXi host.

1. From the direct console, select **Configure Management Network** and press Enter.
2. Select **VLAN** and press Enter.
3. Enter a VLAN ID number from 1 through 4094.

Configuring IP Settings for ESXi

By default, DHCP sets the IP address, subnet mask, and default gateway.

For future reference, write down the IP address.

When you have access to the direct console, you can optionally configure a static network address. The default subnet mask is 255.255.0.0.

Configure IP Settings from the Direct Console

If you have physical access to the host or remote access to the direct console, you can use the direct console to configure the IP address, subnet mask, and default gateway.

1. Select **Configure Management Network** and press Enter.
2. Select **IP Configuration** and press Enter.
3. Select **Set static IP address and network configuration**.
4. Enter the IP address, subnet mask, and default gateway and press Enter.

Configure IP Settings from the vSphere Client

If you do not have physical access to the host, you can use the vSphere Client to configure static IP settings.

1. Log in to the vCenter Server from the vSphere Client.
2. Select the host in the inventory.
3. On the **Configure** tab, expand **Networking**.
4. Select **VMkernel adapters**.
5. Select **vmk0 Management Network** and click the edit icon.
6. Select **IPv4 settings**.
7. Select **Use static IPv4 settings**.
8. Enter or change the static IPv4 address settings.
9. Optional: Set static IPv6 addresses.
   a) Select **IPv6 settings**.
   b) Select **Static IPv6 addresses**.
   c) Click the add icon.
   d) Type the IPv6 address and click **OK**.
10. Click **OK**.

Configuring DNS for ESXi

You can select either manual or automatic DNS configuration of the ESXi host.

The default is automatic. For automatic DNS to work, your network environment must have a DHCP server and a DNS server.

In network environments where automatic DNS is not available or not desirable, you can configure static DNS information, including a host name, a primary name server, a secondary name server, and DNS suffixes.

Configure DNS Settings from the Direct Console
If you have physical access to the host or remote access to the direct console, you can use the direct console to configure DNS information.

1. Select **Configure Management Network** and press Enter.
2. Select **DNS Configuration** and press Enter.
3. Select **Use the following DNS server addresses and hostname**.
4. Enter the primary server, an alternative server (optional), and the host name.

Configure DNS Suffixes
If you have physical access to the host, you can use the direct console to configure DNS information. By default, DHCP acquires the DNS suffixes.

1. From the direct console, select **Configure Management Network**.
2. Select **Custom DNS Suffixes** and press Enter.
3. Enter new DNS suffixes.

Configure the Network Settings on a Host That Is Not Attached to the Network

Some highly secure environments do not permit unconfigured hosts on the network to be powered on. You can configure the host before you attach the host to the network.

Verify that no network cables are connected to the host.

1. Power on the host.
2. Use the direct console user interface to configure the password for the administrator account (root).
3. Use the direct console user interface to configure a static IP address.
4. Connect a network cable to the host.
5. Optional: Use the vSphere Client to connect to a vCenter Server system.
6. Optional: Add the host to the vCenter Server inventory.

Test the Management Network

You can use the direct console to do simple network connectivity tests.

The direct console performs the following tests.

- Pings the default gateway
- Pings the primary DNS name server
- Pings the secondary DNS nameserver
- Resolves the configured host name

1. From the direct console, select **Test Management Network** and press Enter.
2. Press Enter to start the test.

Restart the Management Agents

The management agents synchronize VMware components and let you access the ESXi host by using the vSphere Client and vCenter Server.

The vSphere Client and vCenter Server are installed with the vSphere software. You might need to restart the management agents if remote access is interrupted. Restarting the management agents restarts all management agents

and services that are installed and running in `/etc/init.d` on the ESXi host. Typically, these agents include hostd, ntpd, sfcbd, slpd, wsman, and vobd. The software also restarts the Fault Domain Manager (FDM) if installed.

Users accessing this host by using the vSphere Client and vCenter Server lose connectivity when you restart management agents.

1. From the direct console, select **Troubleshooting Options** and press Enter.
2. Select **Restart Management Agents** and press Enter.
3. Press F11 to confirm the restart.

The ESXi host restarts the management agents and services.

Restart the Management Network

Restarting the management network interface might be required to restore networking or to renew a DHCP lease.

Restarting the management network will result in a brief network outage that might temporarily affect running virtual machines.
If a renewed DHCP lease results in a new network identity (IP address or host name), remote management software will be disconnected.

1. From the direct console, select **Restart Management Network** and press Enter.
2. Press F11 to confirm the restart.

Test Connectivity to Devices and Networks

You can use the direct console to perform some simple network connectivity tests, and specify other devices and networks.

1. From the direct console, select **Test Management Network** and press Enter.
2. Type addresses to ping or another DNS host name to resolve.
3. Press Enter to start the test.

Restoring the Standard Switch

A vSphere Distributed Switch functions as a single virtual switch across all associated hosts.

Verify that your management network is connected to a distributed switch.

Virtual machines can maintain a consistent network configuration as they migrate across multiple hosts. If you migrate an existing standard switch, or virtual adapter, to a Distributed Switch and the Distributed Switch becomes unnecessary or stops functioning, you can restore the standard switch to ensure that the host remains accessible.When you restore the standard switch, a new virtual adapter is created and the management network uplink that is currently connected to Distributed Switch is migrated to the new virtual switch.
You might need to restore the standard switch for the following reasons:

- The Distributed Switch is not needed or is not functioning.
- The Distributed Switch needs to be repaired to restore connectivity to vCenter Server and the hosts need to remain accessible.
- You do not want vCenter Server to manage the host. When the host is not connected to vCenter Server, most Distributed Switch features are unavailable to the host.

1. From the direct console, select **Restore Standard Switch** and press Enter.
   If the host is on a standard switch, this selection is dimmed, and you cannot select it.

2. Press F11 to confirm.

Storage Behavior

When you start ESXi, the host enters an autoconfiguration phase during which system storage devices are configured with defaults.

When you reboot the ESXi host after installing the ESXi image, the host configures the system storage devices with default settings. Starting with ESXi 7.0, you can activate the option autoPartition, which automatically formats all available empty devices with VMFS, except for legacy SD and USB devices. The default is `autoPartition=FALSE`, which formats with VMFS only boot devices with size larger than 128 GB. For more information, see VMware knowledge base article 77009.

CAUTION: ESXi overwrites any disks that appear to be blank. Disks are considered to be blank if they do not have a valid partition table or partitions. If you are using software that uses such disks, in particular if you are using logical volume manager (LVM) instead of, or in addition to, conventional partitioning schemes, ESXi might cause local LVM to be reformatted. Back up your system data before you power on ESXi for the first time.

On the hard drive or USB device that the ESXi host is booting from, the disk-formatting software retains existing diagnostic partitions that the hardware vendor creates. In the remaining space, the software creates the partitions described below.

Partitions Created by ESXi on the Host Drive

For fresh installations, several new partitions are created for the system boot, boot banks, and ESX-OSData. Fresh ESXi installations use GUID Partition Tables (GPT) instead of MSDOS-based partitioning. The installer creates boot banks of varying size depending on the size of the disk. For more information on the scratch partition see About the Scratch Partition.

The installer affects only the installation disk. The installer does not affect other disks of the server. When you install on a disk, the installer overwrites the entire disk. When the installer autoconfigures storage, the installer does not overwrite hardware vendor partitions.

To create the VMFS datastore, the ESXi installer requires a minimum of 128 GB of free space on the installation disk.

You might want to override this default behavior if, for example, you use shared storage devices instead of local storage. To prevent automatic disk formatting, detach the local storage devices from the host under the following circumstances:

- Before you start the host for the first time.
- Before you start the host after you reset the host to the configuration defaults.

To override the VMFS formatting if automatic disk formatting already occurred, you can remove the datastore. See the *vCenter Server and Host Management* documentation.

About the Scratch Partition

For new installations of ESXi, during the autoconfiguration phase, a scratch partition is created as part of the ESX-OSDATA partition.

Note: Partitioning for hosts that are upgraded to ESXi 7.0 and later from earlier versions differs significantly from partitioning for new installations of ESXi. The upgrade process to ESXi 7.0 and later repartitions the boot device and consolidates the original core dump, locker, and scratch partitions into the ESX-OSData volume.

The scratch partition serves to store system logs, which you need when you create a support bundle. If the scratch partition is not present, system logs are stored in a ramdisk. If no scratch partition is created, you can configure one. You can also override the default configuration.

You can create the scratch partition on a remote SAN or NFS-mounted directory.

Set the Scratch Partition from the vSphere Client

If a scratch partition is not set up, you might want to configure one, especially if the host is low on memory. When a scratch partition is not present, system logs are stored in a ramdisk.

The directory to use for the scratch partition must exist on the host.

1. From the vSphere Client, connect to the vCenter Server.
2. Select the host in the inventory.
3. Click the **Configure** tab.
4. Select **System**.
5. Select **Advanced System Settings**.
   The setting **ScratchConfig.CurrentScratchLocation** shows the current location of the scratch partition.
6. In the **ScratchConfig.ConfiguredScratchLocation** text box, enter a directory path that is unique for this host. For example, `/vmfs/volumes/DatastoreUUID/DatastoreFolder`.
7. Reboot the host for the changes to take effect.

Configuring System Logging

ESXi hosts run the syslog service (`vmsyslogd`) that writes messages from system components to log files and can forward messages to syslog collectors.

You can configure the amount and location of the logs. You can also create and apply log filters to modify the logging policy of an ESXi host.

Configure Syslog on ESXi Hosts

You can use the vSphere Client, the VMware Host Client, or the `esxcli system syslog` command to configure the syslog service.

The syslog service receives, categorizes, and stores log messages for analyses that help you take preventive action in your environment.

Set ESXi Syslog by using the vSphere Client
You can use the vSphere Client command to configure the syslog service globally and edit various advanced settings.

1. Browse to the ESXi host in the vSphere Client inventory.
2. Click **Configure**.
3. Under **System**, click **Advanced System Settings**.
4. Click **Edit**.
5. Filter for `syslog`.
6. To set up logging globally and configure various advanced settings, see ESXi Syslog Options.
7. Optional: To overwrite the default log size and log rotation for any of the logs:
   a) Click the name of the log that you want to customize.
   b) Enter the number of rotations and the log size you want.
8. Click **OK**.

Changes to the syslog options take effect.

Note: Syslog parameter settings that you define by using the vSphere Client or VMware Host Client are effective immediately. However, most settings you define by using ESXCLI require an additional command to take effect. For more details, see ESXi Syslog Options.

Set ESXi Syslog by using the vSphere Client
You can use the vSphere Client to configure and edit syslog service parameters on ESXi hosts.

1. In the vSphere Client , under **Host**, click **Manage > System > Advanced settings**.
2. In the **Search** panel, type a syslog setting you want to define. See ESXi Syslog Options.
3. Select the setting and click **Edit option**.
4. Set the value as described in the table of parameters in ESXi Syslog Options.
5. Click **Save**.

Set ESXi Syslog by using ESXCLI
You can configure the syslog service on ESXi hosts by using the ESXCLI command: `esxcli system syslog config set <syslog option>`.

For information about using the esxcli system syslog command and other ESXCLI commands, see Getting Started with ESXCLI. For details how to open the ESXi firewall for the port specified in each remote host specification, see ESXi Firewall Configuration.

Note:

Using ESXCLI requires ESXi to open SSH logins, which is a security risk, and is not recommended. If you chose to use ESXCLI, make sure you use the `esxcli system syslog reload` command after setting each parameter to make sure that it takes effect.

Use the ESXCLI command `esxcli system syslog config set <syslog option>` to set a syslog option that you decide to enable. For example, to set the `Syslog.global.logHost` option, use the command `esxcli system syslog config set --loghost=<str>`

After setting `Syslog.global.logHost`, ESXi hosts open and maintain connections to the syslog collectors, and the transmission of messages begins immediately. When ESXi generates a syslog message, it writes it to the appropriate log file on the ESXi host and also forwards it to all configured syslog collectors.

Fine-tune Syslog on ESXi Hosts

By using the right syslog settings, you can achieve proactive monitoring of your environment, reduce downtime and take preventive action on servers.

While setting up syslog, you need to consider several parameters that affect log file retention, syslog transmission, transmission length, error handling, and the set up of SSL certificates for secure syslog message transmission. What follows are recommendations for fine-tuning your syslog parameters. You can see a description of all available parameters at ESXi Syslog Options.

How to Specify Log File Retention
By default, log files cannot expand past a configured size. Once a log file reaches the configured size, logging is routed to a new log file and the oldest log file is deleted.

Note: Best practice is to balance the rotate and size settings. Increasing the rotate setting ensures that syslog files are generated often enough to prevent any potential corruption or destruction from the other log files. Increasing the size setting reduces the time for switching to another log file. Optimal size settings are a multiple of 1024 KiB.

Use the Syslog.global.defaultSize setting to specify the log file maximum size in KiB, and Syslog.global.defaultRotate to set the maximum number of old log files to keep before rotating to a new log file. To change the log file retention parameters associated with a specific program, use the `Syslog.loggers.<progName>.rotate` and

`Syslog.loggers.<progName>.size settings`, where `<progName>` is the name of the program whose parameters you want to adjust.

Manage Settings that Affect the Virtual Machine Log File

You can configure some settings that affect the virtual machine log file, `vmware.log`, either in the `vmx` file or in the `/etc/vmware/config` file. You must power off a virtual machine to edit the `vmx` file and edits take effect only on that virtual machine. If you use the `/etc/vmware/config` file, you must add the prefix *`"vmx"`* to the setting, for example `vmx.log.keepOld = "20"` , and edits affect all virtual machines on the ESXi host.

Table 22: Configurable settings for the vmware.log file

Parameter	Description	Example	Notes
`logging`	Disables all virtual machine logging.	The default value is `logging = "TRUE"` To disable virtual machine logging: `logging = "FALSE"`	Do not use this setting, because disabling virtual machine logging makes it difficult or impossible to get support for virtual machine problems. If you need to use this setting for some reason, you can only place it in the `vmx` file of a virtual machine.
`log.throttleBytesPerSec`	Controls when a log file throttles. Log file throttling occurs when writes to the `vmware.log` exceed the specified rate for a significant amount of time. This occurs when code within the VMX process, which controls a virtual machine, creates excessive log messages. The default value for this setting is 1 KB/sec. In case of log thottling, you see `<<< Log Throttled >>>` in the `vmware.log` file.	`log.throttleBytesPerSec = "1500"` To disable log throttling, use `log.throttleBytesPerSec = "0xFFFFFFFF"`	Log file thottling might obscure information necessary to diagnose problems with the affected virtual machine. If you need to disable log throttling, place the line in the example in the `vmx` file of the affected virtual machine. Remove the line after the debugging session ends.
`log.keepOld`	Controls the number of older `vmware.log` file to retain.	`log.keepOld = "20"`	Do not put the value of this setting below the default value (10). If virtual machines are frequently modified or moved, consider raising this setting to 20 or more.
`log.rotateSize`	Controls the maximum size of a `vmware.log` file in bytes.	`log.rotateSize = "2500000"` To disable limiting the maximum size of a `vmware.log` file, use `log.rotateSize = "0"`	A value of this setting below 100,000 can cause a loss of critical log messages and affect virtual machine performance. In ESXi 7.x and earlier, the default value of this setting places no limit on the size of a `vmware.log` file. In ESXi 8.x and later, the default value of this setting is 2,048,000.

Parameter	Description	Example	Notes
log.fileName	Controls the name and location of virtual machine log files.	log.fileName = "myVMLog" This setting changes the name of the virtual machine log files from vmware.log to myVMlog. log.fileName = "/vmfs/volumes/vol1/myVM/myVM.log" This setting directs virtual machine log files to a directory on a different VMFS volume (vol1) by using myVM for a file name.	Do not place a log file outside the virtual machine directory to make sure that the collection of host support bundles picks up the log file, which can be critical to debug virtual machine problems.
log.fileLevel	Controls the minimum level at which messages are written to vmware.log. Every log message has a level associated with it. Levels below the specified setting are not added to a virtual machine log file. The virtual machine message log levels (from most to least restricted) are: • error • warning • notice • info (default) • trivia • debug • debug1 • debug2 • debug3 • debug4 • debug5 • debug6 • debug7 • debug8 • debug9 • debug10	log.fileLevel = "debug1"	Do not set a more restrictive level than "info" to avoid filtering out messages that are necessary for debugging virtual machine problems. Lower the level below "info" only upon request by licensed support. Restore the setting to "info" after debugging ends.
log.filter.minLogLevel.<groupName>	Controls the output of specialized debugging messages.	log.filter.minLogLevel.<groupName> = "debug5"	Use this setting only upon request by licensed support, who should provide one or more <groupName> parameters. Remove the setting after debugging ends.
log.sysogID	Activates the sending of virtual machine log messages to the system logger of an ESXi host, such as the syslog.	log.syslogID = "vmx"	Use "vmx" as value for this setting to allow the ESXi syslog daemon, vmsyslogd, to send these messages to a separate log file.

Parameter	Description	Example	Notes
`log.syslogLevel`	Controls the minimum level at which messages are output to the system logger of an ESXi host, such as the syslog.	`log.syslogLevel = "debug"`	The levels and functioning of this setting are identical to those for the `log.fileLevel` setting.

How to Specify Message Transmission to Remote Hosts

Optionally, you can configure ESXi to send syslog messages to one or more remote hosts, called syslog collectors, such as VMware Aria Operations for Logs (formerly VMware vRealize Log Insight and vCenter Log Insight), to collect syslog messages.

Note: Best practice is that you configure each ESXi host to send syslog messages to at least one syslog collector. This helps ensure that the messages are preserved in case of a catastrophic system event and that you can process syslog messages in various ways, such as real-time categorization and analysis (for example, by type, time span, or machine), or archive messages.

Use the `Syslog.global.logHost` setting to define remote host specifications. Separate multiple remote host specifications with a comma (,). After setting `Syslog.global.logHost`, ESXi hosts open and maintain connections to the syslog collectors, and the transmission of messages begins immediately. When ESXi generates a syslog message, it writes it to the appropriate log file on the ESXi host and also forwards it to all configured syslog collectors.

In addition to syslog messages, audit messages can also be transmitted to syslog collectors for security purposes. Audit records track security-related activity on the ESXi host. For more information about audit records, see Audit Records.

Note: Consult with your company security response team if and how to set audit records. Certified configurations usually require audit records to be activated.

What follows is the syntax for `Syslog.global.logHost` remote host specifications:

```
protocol://target[:port]
```

Parameter	Description	Notes
`protocol`	Specifies the networking protocol. Valid values are `udp`, `tcp`, and `ssl`.	The `ssl` protocol specifies that transmission of syslog messages is encrypted. The `tcp` and `udp` protocols do not encrypt the transmission. **Note:** If capturing syslog messages or audit messages is critical to your system, avoid using the `udp` protocol because the networking infrastructure external to ESXi might drop UDP messages.
`target`	Specifies the remote host. You can use either an IPV4 or IPV6 address, or a host name.	When you use an IPV6 address, you must embed it in square brackets `[xxx]`, where `xxx` is the IPV6 address.
`port`	(Optional) Specifies the remote host port to use. If you use UDP or TCP, the default port is 514. If you use SSL, the default port is 1514. If you choose to use different ports from 514 or 1514, you must adjust the ESXi firewall to open the port.	For details how to open the ESXi firewall for the port specified in each remote host specification, see ESXi Firewall Configuration.

Examples of remote machine specifications:

Syslog.global.logHost string example	Notes
tcp://10.176.130.7:12345	Transmits syslog messages to 10.176.130.7 using TCP/IP and port 12345.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]	Transmits syslog messages to an IPV6 address using port 1514.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:5432	Transmit syslog messages to an IPV6 address using port 54321.
udp://company.com	Transmits syslog messages to `company.com` using UDP and port 514.
udp://company.com,tcp://10.20.30.40:1050	Transmits syslog messages to two remote hosts. The first remote host uses UDP to communicate with `company.com` using port 514. The second remote host uses TCP to communicate with the IPV4 address `10.20.30.40` using port 1050.
ssl://company.com	Transmits syslog messages to `company.com` using SSL (TLS) and port 514.

Maximum Message Transmission Length

If you use UDP, the maximum syslog message transmission length is 480 bytes for IPV4 and 1180 bytes for IPV6.

For TCP or SSL, the default maximum syslog message transmission length is 1 kibibyte (KiB). You can increase this length by using the `Syslog.global.remoteHost.maxMsgLen` parameter. The maximum value is 16 KiB. Messages longer than 16 KiB are truncated.

Note: If increasing the maximum transmission length is necessary, best practice is to increase the length only as much as specifically necessary.

Increasing the maximum syslog message length can cause problems if the networking and syslog infrastructure external to ESXi is unable to handle messages longer than 1 KiB.

Note: Best practice is that you do not use UDP to transmit syslog messages due to the packet length constraints and the possibility that the external networking infrastructure might drop the messages.

Considerations for Certificates When Configuring SSL Transmissions to Remote Hosts

When configuring ESXi to transmit syslog messages to remote hosts using SSL, you must add an SSL certificate for each remote host to the ESXi host CA store. For more information, see Certificate Management for ESXi Hosts and Manage CA Certificates with ESXCLI.

Note: Consult with your syslog collector documentation on how to configure the collector for secure receipt of syslog messages using SSL and a private key.

Additional SSL Transmission Parameters

An ESXi system complying with security certification requirements might require activating X509 CRL checks. You turn on the advanced settings `Syslog.global.certificate.strictX509Compliance` and `Syslog.global.certificate.checkCRL` by changing the default value of `false` to `true`. Due to implementation limitations, if you activate CRL checks by using the setting `Syslog.global.certificate.checkSSLCerts`, then all certificates in a certificate chain must provide a CRL link. By default, the setting is active. You can deactivate SSL certificate checks by changing the setting to `false`, but this is not a best practice. You might need to turn off SSL certificate checks when troubleshooting communications with a remote host, but do this only for a limited time.

Where to Find Syslog Daemon Error and Status Information

The ESXi syslog daemon uses the log file `/var/run/log/vmsyslogd.log` to store status and error information, including dropped messages. If audit record transmission is active, the syslog daemon also emits audit records related

to its operation, such as daemon start, stop, and error conditions, which allows you to verify that the syslog daemon runs properly.

How to Change the Default Syslog Log File Storage Area

The default syslog log file storage area is `/var/run/log`, local to each ESXi host. Use the `Syslog.global.logDir` syslog configuration variable to change the default syslog log file storage area, as long as the location resides on persistent storage. If `Syslog.global.logDir` is configured to a persistent store shared by multiple ESXi hosts to store their syslog log files, change the `Syslog.global.logDirUnique` setting to `true` to prevent mixing logs. The `Syslog.global.logDirUnique` setting makes sure that each ESXi machine gets a unique name added to the `Syslog.global.logDir` path, separating the log files from other hosts.

Syslog Message Queueing for Remote Hosts and Message Drops

Once syslog emissions start, they never stop except for ESXi reboots and failures, or a syslog reconfiguration to stop.

To avoid dropping messages, ESXi uses an in-memory queue that allows the `vmsyslogd` service to handle the following conditions for a short time:

- ESXi generates log messages at a faster rate than the `vmsyslogd` service can process and transmit
- Network connectivity between ESXi and the remote host fails

If either of these conditions continues for a long period, the capacity of the in-memory queue might not be sufficient and `vmsyslog` might stop transmitting messages and audit logs to remote hosts. No data is lost, because dropped messages are written to the `/var/run/log/vmsyslogd-dropped.log` file.

To minimize the chance that message dropping occurs, place the `vmsyslogd` log files on the fastest available storage and configure `vmsyslogd` and its syslog collectors on a network with end-to-end bandwidth greater than 1 GigE.

Note: Consider an end-to-end bandwidth of 2.5 GigE or more, preferably 10 GigE, to optimize performance and prevent message drops.

If you see excessive logs from an application, file a support service request for analysis and correction.

You can see statistics about message drops in the syslog daemon log file.

You can see dropped messages at `/var/run/log/vmsyslogd-dropped.log`. This log file has retention settings specific to it, similar to those for the program-specific retention parameters. The dropped messages log file retention parameters are: `Syslog.global.droppedMsgs.fileRotate` and `Syslog.global.droppedMsgs.fileSize`.

ESXi Syslog Options

You can define the behavior of ESXi syslog files and transmissions by using a set of syslog options.

Apart from the base settings, such as `Syslog.global.logHost`, starting from ESXi 7.0 Update 1, a list of advanced options is available for customizations, and NIAP compliance.

Note: Always configure persistent storage before you set any of the audit record parameters or the `Syslog.global.logDir` parameter.

Note: All audit record settings, beginning with `Syslog.global.auditRecord`, take effect immediately. However, for other settings that you define by using ESXCLI, make sure to run the `esxcli system syslog reload` command to enable the changes.

Table 23: Legacy Syslog Options

Option	ESXCLI command	Description
`Syslog.global.logHost`	`esxcli system syslog config set --loghost=<str>`	Defines a comma-delimited list of remote hosts and specifications for message transmissions. If the `loghost=<str>` field is blank, no logs are forwarded. While no hard limit to the number of remote hosts to receive syslog messages exists, good practice is to keep the number of remote hosts to five or less. The format of a remote host specification is: `protocol://hostname|ipv4|'['ipv6']'[:port][?formatter=value[&framing=value]]`. The protocol must be one of `tcp`,`udp`, or `ssl`. The value of a port can be any decimal number between 1 and 65535. If a port is not provided, UDP and TCP use 514; SSL uses 1514. For example: `ssl://hostName1:1514`. The formatter must be RFC_3164 or RFC_5424; RFC_3164 is the default. The framing must be `non_transparent` or `octet_counting`; the default is `non_transparent`. For more information, see Fine-tune Syslog on ESXi Hosts.
`Syslog.global.defaultRotate`	`esxcli system syslog config set --default-rotate=<long>`	Maximum number of old log files to keep. You can set this number globally and for individual subloggers (see `Syslog.global.defaultSize`).
`Syslog.global.defaultSize`	`esxcli system syslog config set --default-size=<long>`	Default size of log files, in KiB. After a file reaches the default size, the syslog service creates a new file. You can set this number globally and for individual subloggers.
`Syslog.global.logDir`	`esxcli system syslog config set --logdir=<str>`	Directory where logs reside. The directory can be on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. Specify the directory as [*datastorename*] *path_to_file*, where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
`Syslog.global.logDirUnique`	`esxcli system syslog config set --logdir-unique=<bool>`	Specifies the ESXi host name to be concatenated to the value of `Syslog.global.logDir`. It is critical that you enable this setting when multiple ESXi hosts log to a shared file system. Selecting this option

Option	ESXCLI command	Description
		creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
`Syslog.global.certificate.checkSSLCerts`	`esxcli system syslog config set --check-ssl-certs=<bool>`	Enforces checking of SSL certificates when transmitting messages to remote hosts.

Table 24: Syslog Options Available Starting from ESXi 7.0 Update 1

Option	ESXCLI command	Description
`Syslog.global.auditRecord.storageCapacity`	`esxcli system auditrecords local set --size=<long>`	Specifies the capacity of the audit record storage directory located on the ESXi host, in MiB. You cannot decrease the capacity of the audit record storage. You can increase the capacity before or after the audit record storage is enabled (see `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.remoteEnable`	`esxcli system auditrecords remote enable`	Enables sending audit records to remote hosts. Remote hosts are specified by using the `Syslog.global.logHost` parameter.
`Syslog.global.auditRecord.storageDirectory`	`esxcli system auditrecords local set --directory=<dir>`	Creates an audit record storage directory and unless specified, sets `/scratch/auditLog` as the default location. You must not manually create an audit record storage directory and you cannot change the audit record storage directory while audit record storage is enabled (see `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.storageEnable`	`esxcli system auditrecords local enable`	Enables the storage of audit records on an ESXi host. If the audit record storage directory does not exist, it is created with the capacity specified by `Syslog.global.auditRecord.storageCapacity`.
`Syslog.global.certificate.checkCRL`	`esxcli system syslog config set --crl-check=<bool>`	Enables checking the revocation status of all the certificates in an SSL certificate chain. Enables verification of X.509 CRLs, which are not checked by default in compliance with industry conventions. A NIAP-validated configuration requires CRL checks. Due to implementation limitations, if CRL checks are enabled, then all certificates in a certificate chain must provide a CRL link. Do not enable the `crl-check` option for installations not related to certification, because of the difficulty in properly configuring an environment that uses CRL checks.

Option	ESXCLI command	Description
Syslog.global.certificate.strictX509Compliance	esxcli system syslog config set --x509-strict=<bool>	Enables strict compliance with X.509. Performs additional validity checks on CA root certificates during verification. These checks are generally not performed, as CA roots are inherently trusted, and might cause incompatibilities with existing, misconfigured CA roots. A NIAP-validated configuration requires even CA roots to pass validations. Do not enable the x509-strict option for installations not related to certification, because of the difficulty in properly configuring an environment that uses CRL checks.
Syslog.global.droppedMsgs.fileRotate	esxcli system syslog config set --drop-log-rotate=<long>	Specifies the number of old dropped message log files to keep.
Syslog.global.droppedMsgs.fileSize	esxcli system syslog config set --drop-log-size=<long>	Specifies the size of each dropped message log file before switching to a new one, in KiB.
Syslog.global.logCheckSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	Enforces checking of SSL certificates when transmitting messages to remote hosts. **Note:** Deprecated. Use Syslog.global.certificate.checkSSLCerts in ESXi 7.0 Update 1 and later.
Syslog.global.logFilters	esxcli system syslog config logfilter [add | remove | set] ...	Specifies one or more log filtering specifications. Each log filter must be separated by a double vertical bar "||". The format of a log filter is: numLogs | ident | logRegexp. numLogssets the maximum number of log entries for the specified log messages. After reaching this number, the specified log messages are filtered and ignored. ident specifies one or more system components to apply the filter to the log messages that these components generate. logRegexp specifies a case-sensitive phrase with Python regular expression syntax to filter the log messages by their content.
Syslog.global.logFiltersEnable		Enables the use of log filters.
Syslog.global.logLevel	esxcli system syslog config set --log-level=<str>	Specifies the log filtering level. You must change this parameter only when troubleshooting an issue with the syslog daemon. You can use the values debug for the most detailed level, info for the default detail level, warning for only warnings or errors, or error, only for errors.

Option	ESXCLI command	Description
`Syslog.global.msgQueueDropMark`	`esxcli system syslog config --queue-drop-mark=<long>)`	Specifies the percent of the message queue capacity at which messages are dropped.
`Syslog.global.remoteHost.connectRetryDelay`	`esxcli system syslog config set --default-timeout=<long>`	Specifies the delay before retrying to connect to a remote host after a connection attempt fails, in seconds.
`Syslog.global.remoteHost.maxMsgLen`	`esxcli system syslog config set --remote-host-max-msg-len=<long>`	For the TCP and SSL protocols, this parameter specifies the maximum length of a syslog transmission before truncation occurs, in bytes. The default maximum length for remote host messages is 1 KiB. You can increase the maximum message length to up to 16 KiB. However, raising this value above 1 KiB does not ensure that long transmissions arrive untruncated to a syslog collector. For example, when the syslog infrastructure that issues a message is external to ESXi. This setting does not affect the UDP protocol. RFC 5426 specifies the UDP message lengths that can be safely accepted at 480 bytes for IPV4 and 1180 bytes for IPV6. Because of these restrictions, and because the networking infrastructure can arbitrary drop UDP packets, the use of UDP for transmitting critical syslog messages is not recommended.
`Syslog.global.vsanBacking`	`esxcli system syslog config set --vsan-backing=<bool>`	Allows log files and the audit record storage directory to be placed on a vSAN cluster. However, enabling this parameter might cause the ESXi host to become unresponsive.

Configure Log Filtering on ESXi Hosts

The log filtering capability lets you modify the logging policy of the syslog service that is running on an ESXi host.

You can create log filters to reduce the number of repetitive entries in the ESXi logs and to denylist specific log events entirely.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Starting with vSphere 7.0 Update 2, you can add log filters and enable log filtering by using ESXCLI. A log filter, once established, remains in place until it is removed, even across ESXi reboots.

Log filters affect all log events that are processed by the ESXi host `vmsyslogd` service, whether they are recorded to a log directory or to a remote syslog server.

You must enable the log filtering capability and reload the syslog daemon to activate the log filters on the ESXi host.

ESXCLI commands to configure log filters follow this pattern: `esxcli system syslog config logfilter {cmd} [cmd options]`.

For example, to get the list of available log filters, run the following command: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter list`.

Use the `set` command to activate or deactivate log filtering: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter set`.

Use the `add` command to add a log filter and the `remove` command to remove a log filter.

Use the `get` command to determine if log filtering is enabled.

A log filter is specified by three components and uses the following syntax: `numLogs | ident | logRegexp`.

Parameter	Description
`numLogs`	Specifies the number of matches of the logRegexp Python regular expression that will be allowed before filtering begins.
`ident`	The `ident` string is how an application identifies itself to the syslog facility. The `logRegexp` filter must be associated with the same application. You can find the `ident` string of an application by inspecting the log files in `/var/run/log`. The third field of each log file begins with the `ident` string and ends with `[`.
`logRegexp`	Python regular expression that identifies the messages which you want to filter out.

For example, to filter out all messages from the hostd daemon that contain the word "mark" after the tenth occurrence, use the following command: `esxcli system syslog config logfilter add --filter="10|Hostd|mark"`.

To remove the log filter, use the command `esxcli system syslog config logfilter remove --filter="10|Hostd|mark"`.

For more information, see ESXi Syslog Options.

Set the Host Image Profile Acceptance Level

The Host Image Profile acceptance level determines which vSphere installation bundles (VIBs) are accepted for installation.

Required privileges: **Host** > **Configuration** > **SecurityProfile** and **Host** > **Configuration** > **Firewall**

VIB signatures are checked and accepted for installation based on a combination of the VIB acceptance level and the host image profile acceptance level. VIBs are tagged with an acceptance level that depends on their signature status.

1. From the vSphere Client, connect to the vCenter Server.
2. Select the host in the inventory.
3. Click the **Configure** tab.
4. Under System, select **Security Profile**.
5. Scroll down to Host Image Profile Acceptance Level, and click **Edit**.
6. Select the acceptance level and click **OK**.

Table 25: Host Image Profile Acceptance Levels

Host Image Profile Acceptance Level	Accepted Levels of VIBs
VMware Certified	VMware Certified

Host Image Profile Acceptance Level	Accepted Levels of VIBs
VMware Accepted	VMware Certified, VMware Accepted
Partner Supported	VMware Certified, VMware Accepted, Partner Supported
Community Supported	VMware Certified, VMware Accepted, Partner Supported, Community Supported

Remove All Custom Packages on ESXi

After adding custom packages, you might decide to remove them.

Before you remove custom packages, shut down or migrate running virtual machines off of the ESXi host.

1. Reboot the ESXi host.
2. In the direct console, select **Remove Custom Extensions** and press F11 to confirm.
3. Reboot the host.

All custom packages are removed.

Modify ESXi Configuration Files

You can modify ESXi configuration files in the ESXi Configuration Store (ConfigStore) by using the `/bin/configstorecli` tool.

The goal of the ESXi Shell tool `configstorecli`, introduced in ESXi 7.0 Update 1, is to manage all configurations for an ESXi host centrally, instead of using different methods and a variety of configuration files.

For more information on how to manage ConfigStore, see VMware knowledge base articles 82227 and 93720.

Deactivate Support for Non-ASCII Characters on ESXi

You can deactivate support for non-ASCII characters for virtual machine files and directory names by using two methods, depending on the ESXi version.

By default, ESXi supports the use of non-ASCII characters for virtual machine file and directory names.

If you need to deactivate support for non-ASCII characters, for ESXi 7.0 Update 2 and later, see VMware knowledge base articles 82227 and 93720.

Prior to ESXi 7.0 Update 2, you can deactivate this support by modifying the `/etc/vmware/hostd/config.xml` file with the following steps:

1. Using a text editor, open the `/etc/vmware/hostd/config.xml` file for the ESXi host.
2. Within the `<config></config>` tag, add the following code.
   ```
   <g11nSupport>false</g11nSupport>
   ```
3. Save and close the file.
4. Reboot the host.

   After you deactivate this support, you can still enter non-ASCII characters for virtual machine names. vSphere user interfaces display the virtual machine names in the non-ASCII characters, but ESXi converts the actual file and directory names to ASCII strings.

Reset the System Configuration

If you are having trouble determining the source of a problem with your ESXi host, you can reset the system configuration.

Before resetting the configuration, back up your ESXi configuration in case you want to restore your configuration.

Changes in the system configuration can be related to various problems, including problems with connectivity to the network and devices. Resetting the system configuration might solve such problems. If resetting the system configuration does not solve the problem, it can still rule out configuration changes made since the initial setup as the source of the problem.

When you reset the configuration, the software overrides all your configuration changes, deletes the password for the administrator account (root), and reboots the host. Configuration changes made by your hardware vendor, such as IP address settings and license configuration, might also be deleted.

Resetting the configuration does not remove virtual machines on the ESXi host. After you reset the configuration defaults, the virtual machines are not visible, but you make them visible again by reconfiguring storage and reregistering the virtual machines.

CAUTION: When you reset the configuration defaults, users accessing the host lose connectivity.

1. Back up the configuration by using the `Get-VMHostFirmware`PowerCLI cmdlet.
2. From the direct console, select **Reset System Configuration** and press Enter.
3. Press F11 to confirm.

The system reboots after all settings are reset to the default values.

After You Install and Set Up ESXi

After you install and set up ESXi, you can use manage hosts by various interfaces, license the hosts, and back up your configuration.

After ESXi is installed and set up, you can manage the host by using the vSphere Client and vCenter Server, license the host, and back up your ESXi configuration. You can also use the VMware Host Client to connect directly to the ESXi host and to manage it. For information about installing and using the VMware Host Client, see *vSphere Single Host Management*.

Note: When you install a standalone ESXi host with TMP enabled that is not connected to a vCenter Server instance, create a backup of the ESXi configuration recovery key. To get the recovery key, run the command `esxcli system settings encryption recovery list` on the ESXi host and note it down. It is possible that the host might not be able to complete booting due to host configuration encryption related problems and in such cases, you can restore the host configuration by using the recovery key and running the configuration recovery process.

For best practices and VMware recommendations, see Best Practices for Secure ESXi Configuration.

Licensing ESXi Hosts

After you install ESXi, it has a 60-day evaluation period during which you can explore the full set of vSphere features provided with a vSphere Enterprise Plus license. You must assign the host an appropriate license before the evaluation period expires.

ESXi hosts are licensed with vSphere licenses that have per-CPU capacity. To license hosts correctly, you must assign them a vSphere license that has enough CPU capacity to cover all CPUs in the hosts. The license must support all features that the hosts are using. For example, if the hosts are connected to a vSphere Distributed Switch, you must assign a license that has the vSphere Distributed Switch feature.

You can use one of following methods to license ESXi hosts:

- License multiple hosts at a time by using the license management function in the vSphere Client. The hosts must be connected to a vCenter Server system. For more information, see *vCenter Server and Host Management*.
- Set up bulk licensing by using PowerCLI commands. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with Auto Deploy. See Set Up Bulk Licensing
- License individual ESXi hosts by using a direct connection with the VMware Host Client. For information about assigning a license key to an ESXi host, see *vSphere Single Host Management*.

Recording the License Key of an ESXi Host

If a host becomes inaccessible or unbootable, you should have a record of its license key. You can write down the license key and tape it to the server, or put the license key in a secure location. You can access the license key from the direct console user interface or the vSphere Client.

View the License Keys of ESXi Hosts from the vSphere Client

You can view the license keys of the hosts that are connected to a vCenter Server system through the vSphere Client.

1. In the vSphere Client, select **Administration**.
2. Under Licensing, select **Licenses**.
3. On the **Assets** tab, select **Hosts**.
4. In the License column, click a license.

You view information about the license, such as its usage and license key.

Access the ESXi License Key from the Direct Console

If you have physical access to the host or remote access to the direct console, you can use the direct console to access the ESXi license key.

- From the direct console, select **View Support Information**.

  The license key appears in the form XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, labeled License Serial Number.

  Note: The physical machine serial number also appears, labeled Serial Number. Do not confuse the license key with the physical machine serial number.

View System Logs

System logs provide detailed information about system operational events.

1. From the direct console, select **View System Logs**.
2. Press a corresponding number key to view a log.

   vCenter Server Agent (vpxa) logs appear if you add the host to vCenter Server.
3. Press Enter or the spacebar to scroll through the messages.
4. Perform a regular expression search.
   a) Press the slash key (/).
   b) Type the text to find.
   c) Press Enter.

   The found text is highlighted on the screen.
5. Press q to return to the direct console.

See also Configure Syslog on ESXi Hosts.

Troubleshooting ESXi Booting

The ESXi booting troubleshooting topics provide solutions to problems that you might encounter during the ESXi booting.

- Host Stops Unexpectedly at Bootup When Sharing a Boot Disk with Another Host
- Host Fails to Boot After You Install ESXi in UEFI Mode

Host Stops Unexpectedly at Bootup When Sharing a Boot Disk with Another Host

When more than one host, either physical or virtual, boots from the same shared physical disk or LUN, they cannot use the same scratch partition.

The host stops at bootup when sharing a boot disk with another host.

More than one ESXi host can share the same physical disk or LUN. When two such hosts also have the same scratch partition configured, either of the hosts can fail at bootup.

1. Set the hosts to boot sequentially, and boot the hosts.
   This setting lets you start the hosts so that you can change the scratch partition for one of them.
2. From the vSphere Client, connect to the vCenter Server.
3. Select the host in the inventory.
4. Click the **Configure** tab.
5. Under System, select **Advanced System Settings**.
6. Select **ScratchConfig**.
   The **ScratchConfig.CurrentScratchLocation** text box shows the current location of the scratch partition.
7. In the **ScratchConfig.ConfiguredScratchLocation** text box, enter a directory path that is unique for this host. For example, `/vmfs/volumes/`*`DatastoreUUID`*`/`*`DatastoreFolder`*.
8. Reboot the host for the changes to take effect.

Host Fails to Boot After You Install ESXi in UEFI Mode

After you install ESXi on a host machine in UEFI mode, the machine might fail to boot.

When you install or upgrade ESXi, the installer tries to create an UEFI boot option named VMware ESXi and make it the default boot option. When you reboot after installing ESXi the reboot might fail. This problem is accompanied by an error message similar to `No boot device available.`

- When the installer creates the UEFI boot option, a problem occurs while writing to the NVRAM on the host motherboard.
- The host firmware does not recognize the attempt to set the UEFI boot option as the first boot option, or the firmware overrides the boot order.
- The boot disk has an MBR or MSDOS partition table. Due to a technical limitation, the UEFI boot option is only created for a GUID Partition Table (GPT) partition table.

Note: UEFI firmware attempts to load the boot image from the EFI system partition, which is FAT based, on the disk. Booting from the EFI system partition only works if the disk is laid out by using a GPT. If the boot disk has an MBR or

MSDOS partition table, a UEFI boot fails. You cannot add a boot entry for MBR. If the disk is fully consumed by ESXi, it cannot be converted to GPT, and you must boot in legacy BIOS mode.

1. While the error message is displayed on screen, open the boot options menu. Depending on your system, the boot options menu might open with a keyboard shortcut, in the BIOS menu, or in a BMC, iLO or iDRAC interface.
2. Check if a boot option VMware ESXi exists and try to boot from it. If the boot is successful, change the boot order and set VMware ESXi as the first boot option.
3. If the problem is not resolved, select an option similar to **Add boot option**.
   The wording and location of the option might vary, depending on your system.
4. Select the file `\EFI\BOOT\BOOTx64.EFI` on the disk that you installed ESXi on.
5. Change the boot order so that the host boots from the option that you added.

Decommission an ESXi Host

If you do not want your server to be an ESXi host, you can decommission the ESXi host machine.

1. Remove VMFS datastores on the internal disks so that the internal disks are no longer set up to store virtual machines.
2. Change the boot setting in the BIOS so that the host no longer boots into ESXi.
   If you installed ESXi in UEFI mode, delete the boot option VMware ESXi or any other boot option created manually.
3. Install another operating system in its place.

ESXi Upgrade

VMware ESXi Upgrade describes how to upgrade VMware ESXi™ to the current version.

About VMware ESXi Upgrade

VMware ESXi Upgrade describes how to upgrade VMware ESXi™ to the current version.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we have updated this guide to remove instances of non-inclusive language.

Intended Audience

VMware ESXi Upgrade is for anyone who needs to upgrade from earlier versions of ESXi. These topics are for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

vCenter Server Upgrade Options

vCenter Server7.0 provides many options for upgrading your vCenter Server deployment. For a successful vCenter Server upgrade, you must understand the upgrade options, the configuration details that impact the upgrade process, and the sequence of tasks.

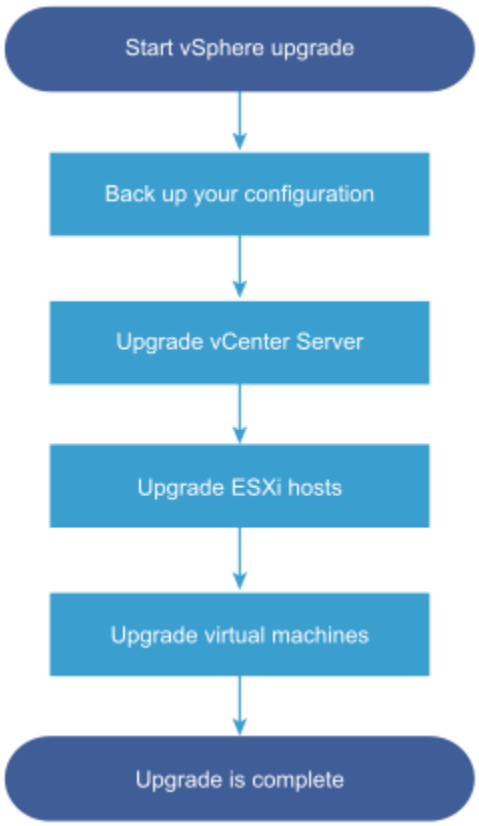
The two core components of vSphere are VMware ESXi™ and VMware vCenter Server™. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. You use the vCenter Server system to pool and manage the resources of multiple hosts. vCenter Server appliance is a preconfigured virtual machine optimized to run vCenter Server.

You can upgrade existing vCenter Server deployments that include either an embedded or an external Platform Services Controller to a deployment consisting of a vCenter Server appliance.

Overview of the vSphere Upgrade Process

vSphere is a sophisticated product with multiple components to upgrade. Understanding the required sequence of tasks is vital for a successful vSphere upgrade.

Figure 12: Overview of vSphere Upgrade Tasks



Upgrading vSphere includes the following tasks:

1. Read the vSphere release notes.
2. Verify that you have backed up your configuration.
3. If your vSphere system includes VMware solutions or plug-ins, verify that they are compatible with the vCenter Server appliance version to which you are upgrading. See *VMware Product Interoperability Matrix* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
4. Upgrade vCenter Server.
5. To ensure sufficient disk storage for log files, consider setting up a syslog server for remote logging. Setting up logging on a remote host is especially important for hosts with a limited amount of local storage.
6. Upgrade your VMs manually or by using vSphere Lifecycle Manager to perform an orchestrated upgrade.

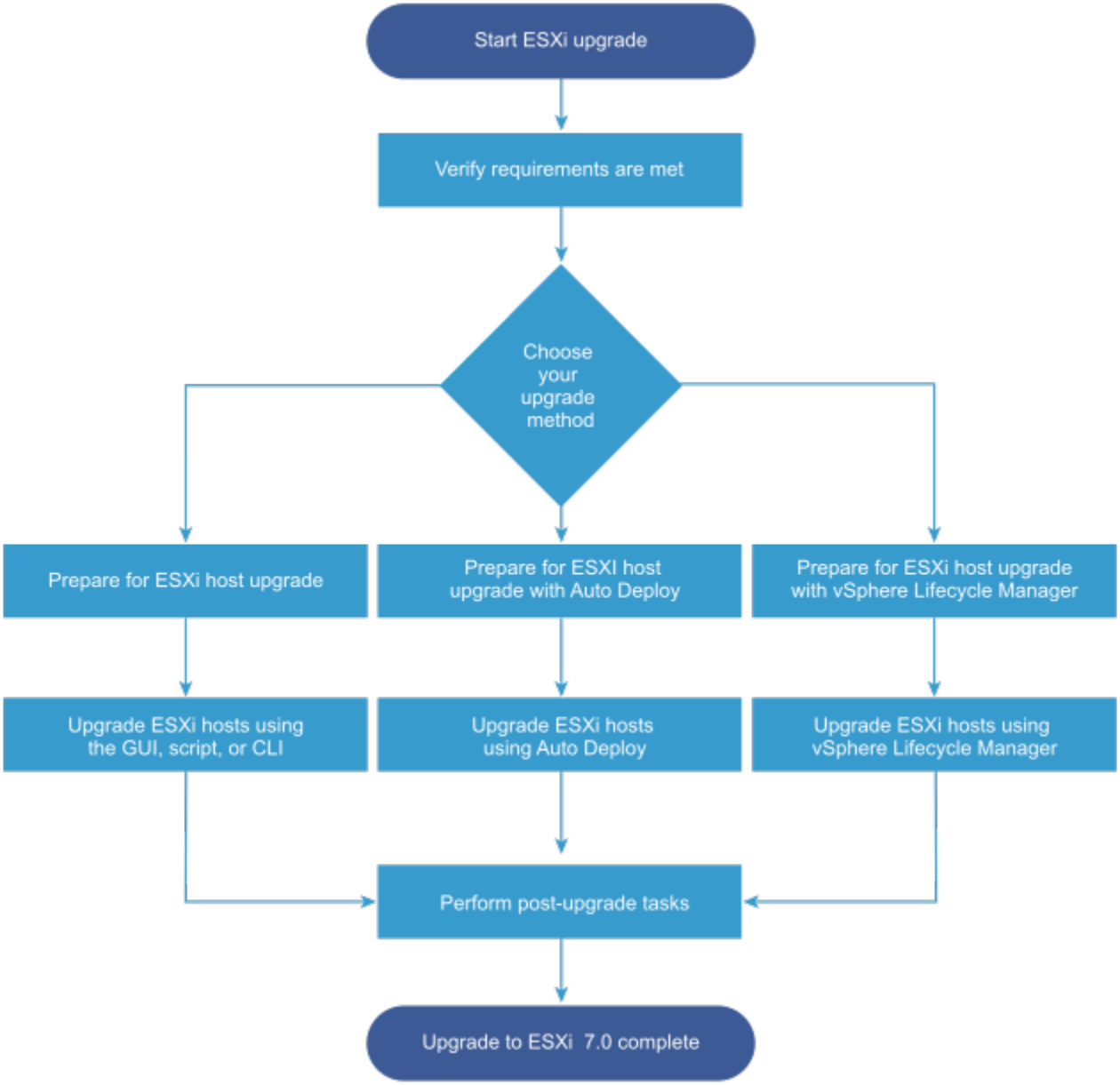
Overview of the ESXi Host Upgrade Process

VMware provides several ways to upgrade ESXi hosts with version 6.5 and version 6.7 to ESXi version 7.0.

The details and level of support for an upgrade to ESXi7.0 depend on the host to be upgraded and the upgrade method that you use. Verify that the upgrade path from your current version of ESXi to the version to which you are upgrading, is supported. For more information, see the VMware Product Interoperability Matrices at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

You can upgrade an ESXi host with version 6.5 or 6.7 by using an interactive upgrade from a CD, DVD, or USB, a scripted upgrade, ESXCLI, or vSphere Lifecycle Manager. When you upgrade an ESXi 6.5 or 6.7 host that has custom VIBs to version 7.0, all supported custom VIBs are migrated.For more information, see Upgrading Hosts That Have Third-Party Custom VIBs.

Figure 13: Overview of the ESXi Host Upgrade Process



The following high-level steps are for upgrading ESXi.

1. Verify that your system meets the upgrade requirements. See ESXi Requirements.
2. Prepare your environment before upgrading. See Before Upgrading ESXi Hosts.
3. Determine where you want to locate and boot the ESXi installer. See Media Options for Booting the ESXi Installer. If you are network booting the installer, verify that your network boot infrastructure is properly set up. See Network Booting the ESXi Installer.
4. Upgrade ESXi. See Upgrading ESXi Hosts
5. After upgrading ESXi hosts, you must reconnect the hosts to the vCenter Server and reapply the licenses. See After You Upgrade ESXi Hosts.

The following methods are supported for a direct upgrade to ESXi7.0.

- Use the interactive graphical user interface (GUI) installer from a CD, DVD, or USB drive.
- Perform a scripted upgrade.
- Use ESXCLI.
- Use vSphere Auto Deploy. If the ESXi host is deployed by using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with a 7.0 image.
- Use the vSphere Lifecycle Manager.

Graphical User Interface (GUI) Installer	You can upgrade interactively by using an ESXi installer ISO image on a CD, DVD, or USB flash drive or by network booting the installer. This method is appropriate for deployments with a few hosts. If during the installation process, you select a target disk that contains an ESXi installation, the installer upgrades the host to ESXi version 7.0. The installer also gives you the option to migrate some existing host settings and configuration files and to preserve the existing VMFS datastore. See Upgrade Hosts Interactively.
Perform a Scripted Upgrade	To do a scripted upgrade, you can use the ESXi7.0 installer from a CD, DVD, or USB flash drive or by network booting the installer. This method is an efficient way to deploy multiple hosts. For more information, see Installing or Upgrading Hosts by Using a Script.
ESXCLI	You can use ESXCLI to upgrade ESXi 6.5 hosts or ESXi6.7 hosts to ESXi7.0 hosts. See Upgrading Hosts by Using ESXCLI Commands .
vSphere Auto Deploy	If an ESXi host is deployed with vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host and reboot it with a new image profile. Such profile contains an ESXi upgrade or patch, a host configuration profile, and optionally, third-party drivers or management agents that are provided by VMware partners. You can build custom images by using vSphere ESXi Image Builder CLI. For more information, see Using vSphere Auto Deploy to Reprovision Hosts.
vSphere Lifecycle Manager	vSphere Lifecycle Manager is a vCenter Server service for installing, upgrading, and updating ESXi hosts. By using images and baselines, vSphere Lifecycle Manager enables centralized and simplified lifecycle management for multiple ESXi hosts at a cluster level. For more information about performing orchestrated installations, upgrades, and updates, see the Managing Host and Cluster Lifecycle documentation.

Upgrading Virtual Machines and VMware Tools

After you upgrade an ESXi host, you can upgrade the virtual machines on the host to take advantage of new features.

You have the following tools for upgrading virtual machines.

vSphere Client	You can use the vSphere Client to upgrade a virtual machine step by step. For more information about upgrading virtual machines, see the *vSphere Virtual Machine Administration* documentation.
vSphere Lifecycle Manager	You can use the vSphere Lifecycle Manager to upgrade the virtual machine hardware and VMware Tools versions of the virtual machines in your environment. The vSphere Lifecycle Manager automates the upgrade process and verifies that the steps occur in the correct order. For more information, see the *Managing Host and Cluster Lifecycle* documentation.

Upgrading ESXi Hosts

After you upgrade vCenter Server, upgrade your ESXi hosts. You can upgrade ESXi 6.5 and 6.7 hosts directly to ESXi7.0.

To upgrade hosts, you can use the tools and methods that are described in Overview of the ESXi Host Upgrade Process.

CAUTION: If you upgrade hosts managed by vCenter Server, you must upgrade vCenter Server before you upgrade the ESXi hosts. If you do not upgrade your environment in the correct order, you can lose data and lose access to servers.

ESXi Requirements

To install or upgrade ESXi, your system must meet specific hardware and software requirements.

- ESXi System Storage Overview
- ESXi Hardware Requirements
- Supported Remote Management Server Models and Firmware Versions
- Recommendations for Enhanced ESXi Performance
- Incoming and Outgoing Firewall Ports for ESXi Hosts
- Required Free Space for System Logging
- VMware Host Client System Requirements
- ESXi Passwords and Account Lockout

ESXi System Storage Overview

ESXi7.0 introduces a system storage layout that allows flexible partition management and support for large modules, and third-party components, while facilitating debugging.

ESXi7.0 System Storage Changes

Before ESXi7.0 , partition sizes were fixed, except for the `/scratch` partition and the optional VMFS datastore, and the partition numbers were static, limiting partition management. With ESXi7.0, partitions are consolidated into fewer, larger partitions that are expandable, depending on the used boot media and its capacity.

The ESXi7.0 system storage layout consists of four partitions:

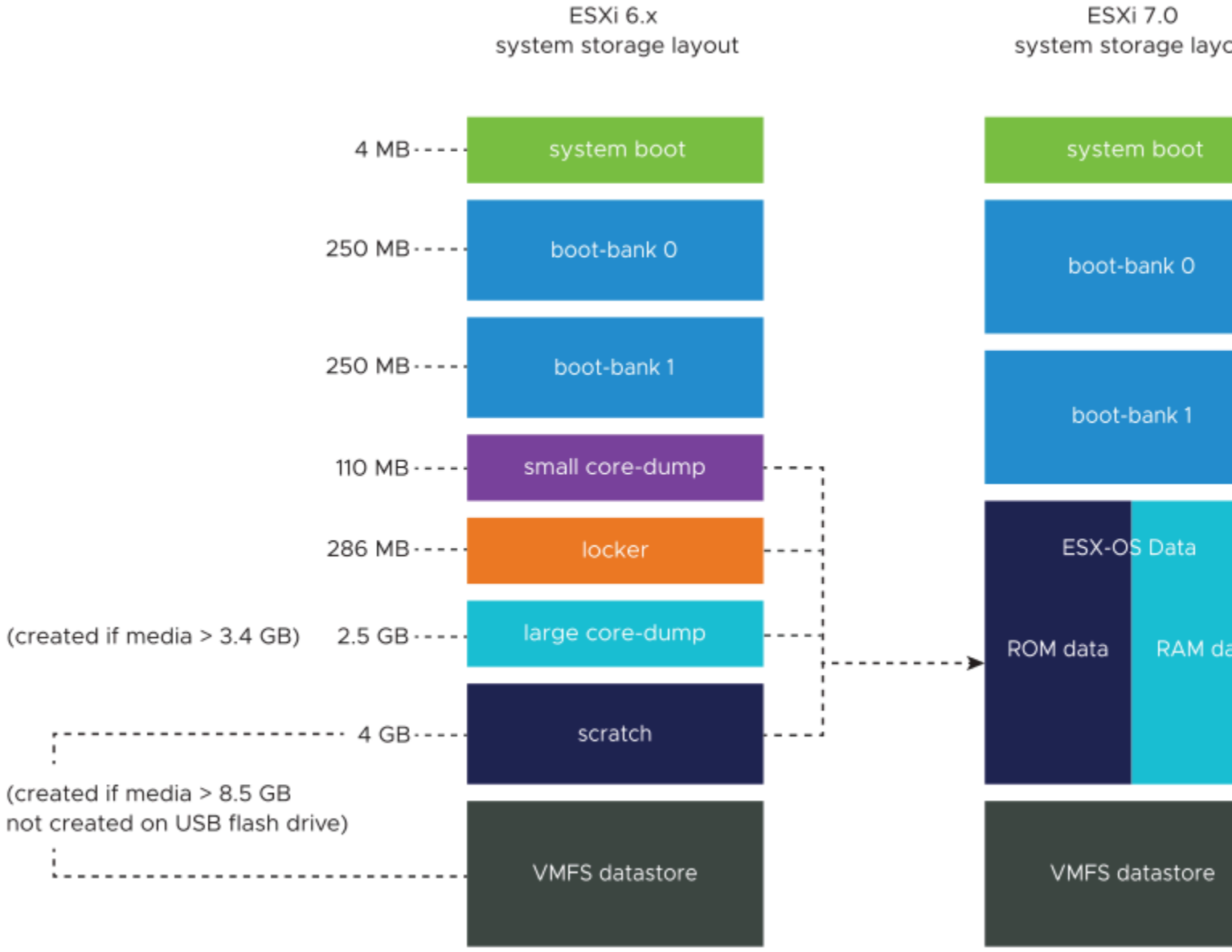
Table 26: ESXi 7.0 system storage partitions:

Partition	Use	Type
System Boot	Stores boot loader and EFI modules.	FAT16
Boot-bank 0	System space to store ESXi boot modules.	FAT16
Boot-bank 1	System space to store ESXi boot modules.	FAT16
ESX-OSData	Acts as the unified location to store additional modules. Not used for booting and virtual machines. Consolidates the legacy `/scratch` partition, locker partition for VMware Tools, and core dump destinations. **CAUTION:** Always create ESX-OSData partitions on persistent storage device that is not shared between ESXi hosts. Use USB, SD and non-USB flash media devices only for boot bank partitions.	VMFS-L

The ESX-OSData volume is divided into two high-level categories of data, persistent and non-persistent data. Persistent data contains of data written infrequently, for example, VMware Tools ISOs, configurations, and core dumps.

Non-persistent data contains of frequently written data, for example, logs, VMFS global traces, vSAN Entry Persistence Daemon (EPD) data, vSAN traces, and real-time databases.

Figure 14: Consolidated system storage in ESXi 7.0 and later



ESXi7.0 System Storage Sizes

Partition sizes, except for the system boot partition, can vary depending on the size of the boot media used. If the boot media is a high-endurance one with capacity larger than 142 GB, a VMFS datastore is created automatically to store virtual machine data.

You can review the boot media capacity and the automatic sizing as configured by the ESXi installer by using the vSphere Client and navigating to the **Partition Details** view. Alternatively, you can use ESXCLI, for example the `esxcli storage filesystem list` command.

Table 27: ESXi7.0 System Storage Sizes, Depending on the Used Boot Media and Its Capacity.

Boot Media Size	8-10 GB	10-32 GB	32-128 GB	>128 GB
System Boot	100 MB	100 MB	100 MB	100 MB
Boot-bank 0	500 MB	1 GB	4 GB	4 GB
Boot-bank 1	500 MB	1 GB	4 GB	4 GB
ESX-OSData	remaining space	remaining space	remaining space	up to 128 GB
VMFS datastore				remaining space for media size > 142 GB

Starting with vSphere 7.0 Update 1c, you can use the ESXi installer boot option `systemMediaSize` to limit the size of system storage partitions on the boot media. If your system has a small footprint that does not require the maximum of 128 GB of system storage size, you can limit it to the minimum of 32 GB. The `systemMediaSize` parameter accepts the following values:

- min (32 GB, for single disk or embedded servers)
- small (64 GB, for servers with at least 512 GB of RAM)
- default (128 GB)
- max (consume all available space, for multi-terabyte servers)

The selected value must fit the purpose of your system. For example, a system with 1 TB of memory must use the minimum of 64 GB for system storage. To set the boot option at install time, for example `systemMediaSize=small` , refer to Enter Boot Options to Start an Installation or Upgrade Script. For more information, see Knowledge Base article 81166.

ESXi7.0 System Storage Links

The sub-systems that require access to the ESXi partitions, access these partitions by using the following symbolic links:

Table 28: ESXi7.0 system storage symbolic links.

System Storage Volume	Symbolic Link
Boot-bank 0	`/bootbank`
Boot-bank 1	`/altbootbank`

Persistent data	`/productLocker`
	`/locker`
	`/var/core`
	`/usr/lib/vmware/isoimages`
	`/usr/lib/vmware/floppies`

Non-persistent data	`/var/run`
	`/var/log`
	`/var/vmware`
	`/var/tmp`
	`/scratch`

ESXi Hardware Requirements

Make sure that the host meets the minimum hardware configurations supported by ESXi7.0.

Hardware and System Resources

To install or upgrade ESXi, your hardware and system resources must meet the following requirements:

- Supported server platform. For a list of supported platforms, see the VMware Compatibility Guide.
- ESXi7.0 requires a host with at least two CPU cores.
- ESXi7.0 supports a broad range of multi-core of 64-bit x86 processors. For a complete list of supported processors, see the VMware Compatibility Guide.
- ESXi7.0 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi7.0 requires a minimum of 8 GB of physical RAM. Provide at least 8 GB of RAM to run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs.
- One or more Gigabit or faster Ethernet controllers. For a list of supported network adapter models, see the VMware Compatibility Guide.
- ESXi7.0 requires a boot disk of at least 32 GB of persistent storage such as HDD, SSD, or NVMe. Use USB, SD and non-USB flash media devices only for ESXi boot bank partitions. A boot device must not be shared between ESXi hosts.
- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks are considered remote, not local. These disks are not used as a scratch partition by default because they are seen as remote.

  Note: You cannot connect a SATA CD-ROM device to a virtual machine on an ESXi host. To use the SATA CD-ROM device, you must use IDE emulation mode.

Storage Systems

For a list of supported storage systems, see the VMware Compatibility Guide. For Software Fibre Channel over Ethernet (FCoE), see Installing and Booting ESXi with Software FCoE.

ESXi Booting Requirements

vSphere 7.0 supports booting ESXi hosts from the Unified Extensible Firmware Interface (UEFI). With UEFI, you can boot systems from hard drives, CD-ROM drives, or USB media.

vSphere Auto Deploy supports network booting and provisioning of ESXi hosts with UEFI.

ESXi can boot from a disk larger than 2 TB if the system firmware and the firmware on any add-in card that you are using support it. See the vendor documentation.

Storage Requirements for ESXi7.0 Installation or Upgrade

For best performance of an ESXi7.0 installation, use a persistent storage device that is a minimum of 32 GB for boot devices. Upgrading to ESXi7.0 requires a boot device that is a minimum of 8 GB. When booting from a local disk, SAN or iSCSI LUN, at least a 32 GB disk is required to allow for the creation of system storage volumes, which include a boot partition, boot banks, and a VMFS-L based ESX-OSData volume. The ESX-OSData volume takes on the role of the legacy `/scratch` partition, locker partition for VMware Tools, and core dump destination.

Other options for best performance of an ESXi7.0 installation are the following:

- A local disk of 128 GB or larger for optimal support of ESX-OSData. The disk contains the boot partition, ESX-OSData volume and a VMFS datastore.
- A device that supports the minimum of 128 terabytes written (TBW).
- A device that delivers at least 100 MB/s of sequential write speed.
- To provide resiliency in case of device failure, a RAID 1 mirrored device is recommended.

Legacy SD and USB devices are supported with the following limitations:

- SD and USB devices are supported for boot bank partitions. For best performance, also provide a separate persistent local device with a minimum of 32 GB to store the `/scratch` and VMware Tools partitions of the ESX-OSData volume. The optimal capacity for persistent local devices is 128 GB. The use of SD and USB devices for storing ESX-OSData partitions is being deprecated.
- Starting with ESXi 7.0 Update 3, if the boot device is a USB or SD card with no local persistent storage, such as HDD, SSD, or a NVMe device, the VMware Tools partition is automatically created on the RAM disk. For more information, see Connection to the /bootbank partition intermittently breaks when you use USB or SD devices.
- If you assign the `/scratch` partition to a USB or SD card with no local persistent storage, you see warnings to prevent you from creating or configuring partitions other than the boot bank partitions on flash media devices. For best performance, set the `/scratch` partition on the RAM disk. You can also configure and move the `/scratch` partition to a SAN or NFS. For more information, see Creating a persistent scratch location for ESXi 8.x/7.x/6.x.
- You must use an SD flash device that is approved by the server vendor for the particular server model on which you want to install ESXi on an SD flash storage device. You can find a list of validated devices on partnerweb.vmware.com.
- See SD card/USB boot device revised guidance on updated guidance for SD card or USB-based environments.
- To chose a proper SD or USB boot device, see Boot device guidance for low endurance media (vSphere and vSAN).

CAUTION:

If a local disk cannot be found, or the boot media is a USB or SD device without an additional durable storage for persistent data, then the `/scratch` partition is on the RAM disk, linked to `/tmp`, and ESXi7.0 operates in degraded mode.

When in degraded mode, you see a System Alert such as: `ALERT: No persistent storage available for system logs and data. ESX is operating with limited system storage space, logs and system data will be lost on reboot.`

When ESXi7.0 operates in degraded mode, the consumption of RAM for logs might result in nonpersistent logs, possible failure to log or out of memory condition for temporary data. A possible side effect is slow booting due to the time spent for rebuilding of the disk state.

Use persistent storage of sufficient size to prevent degraded mode. You can reconfigure `/scratch` to use a separate disk or LUN.

The upgrade process to ESXi7.0 repartitions the boot device and consolidates the original core dump, locker, and scratch partitions into the ESX-OSData volume.

The following events occur during the repartitioning process:

- If a custom core dump destination is not configured, then the default core dump location is a file in the ESX-OSData volume.
- If the syslog service is configured to store log files on the 4 GB VFAT scratch partition, the log files in `var/run/log` are migrated to the ESX-OSData volume.
- VMware Tools are migrated from the locker partition and the partition is wiped.
- The core dump partition is wiped. The application core dump files that are stored on the scratch partition are deleted.

Note: Rollback to an earlier version of ESXi is not possible due to the repartitioning process of the boot device. To use an earlier version of ESXi after upgrading to version 7.0, you must create a backup of the boot device before the upgrade, and restore the ESXi boot device from the backup.

If you use USB or SD devices to perform an upgrade, the installer attempts to allocate an ESX-OSData region on an available local disk. A datastore is used for `/scratch`, if no space is available. If no local disk or datastore is found, `/scratch` is placed on the RAM disk. After the upgrade, reconfigure `/scratch` to use a persistent datastore or add a new disk for system storage volumes.

After upgrading to ESXi7.0, you can add a new local disk and enable the setting `autoPartition=TRUE` . After a reboot, the boot disk is partitioned. For more information on the boot options to configure the size of ESXi system partitions, see Boot option to configure the size of ESXi system partitions.

In Auto Deploy installations, the installer attempts to allocate a scratch region on an available local disk or datastore. If no local disk or datastore is found, the `/scratch` partition is placed on the RAM disk. Reconfigure `/scratch` to use a persistent datastore after the installation.

For environments that boot from a SAN or use Auto Deploy, the ESX-OSData volume for each ESXi host must be set up on a separate SAN LUN. However, if `/scratch` is configured not to use ESX-OSData, you do not need to allocate a separate LUN for `/scratch` for each host. You can co-locate the scratch regions for multiple ESXi hosts onto a single LUN. The number of hosts assigned to any single LUN should be weighed against the LUN size and the I/O behavior of the virtual machines.

Supported Remote Management Server Models and Firmware Versions

You can use remote management applications to install or upgrade ESXi, or to manage hosts remotely.

Table 29: Supported Remote Management Server Models and Minimum Firmware Versions

Remote Management Server Model	Firmware Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
HP ILO 3	1.28	1.7.0_60-b19
HP ILO 4	1.13	1.7.0_60-b19
HP ILO 5	2.15	N/A
IBM RSA 2	1.03, 1.2	1.6.0_22

Recommendations for Enhanced ESXi Performance

To enhance performance, install or upgrade ESXi on a robust system with more RAM than the minimum required and with multiple physical disks.

For ESXi system requirements, see ESXi Hardware Requirements.

Table 30: Recommendations for Enhanced Performance

System Element	Recommendation
RAM	ESXi hosts require more RAM than typical servers. Provide at least 8 GB of RAM to take full advantage of ESXi features and run virtual machines in typical production environments. An ESXi host must have sufficient RAM to run concurrent virtual machines. The following examples are provided to help you calculate the RAM required by the virtual machines running on the ESXi host.

System Element	Recommendation
	Operating four virtual machines with Red Hat Enterprise Linux or Windows XP requires at least 3 GB of RAM for baseline performance. This figure includes 1024 MB for the virtual machines, 256 MB minimum for each operating system as recommended by vendors. Running these four virtual machines with 512 MB RAM requires that the ESXi host have 4 GB RAM, which includes 2048 MB for the virtual machines. These calculations do not include possible memory savings from using variable overhead memory for each virtual machine. See *vSphere Resource Management*.
Dedicated Fast Ethernet adapters for virtual machines	Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.
Disk location	Place all data that your virtual machines use on physical disks allocated specifically to virtual machines. Performance is better when you do not place your virtual machines on the disk containing the ESXi boot image. Use physical disks that are large enough to hold disk images that all the virtual machines use.
VMFS6 partitioning	The ESXi installer creates the initial VMFS volumes on the first blank local disk found. To add disks or modify the original configuration, use the vSphere Client. This practice ensures that the starting sectors of partitions are 64K-aligned, which improves storage performance. **Note:** For SAS-only environments, the installer might not format the disks. For some SAS disks, it is not possible to identify whether the disks are local or remote. After the installation, you can use the vSphere Client to set up VMFS.
Processors	Faster processors improve ESXi performance. For certain workloads, larger caches improve ESXi performance.
Hardware compatibility	Use devices in your server that are supported by ESXi 7.0 drivers. See the *Hardware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Incoming and Outgoing Firewall Ports for ESXi Hosts

Open and close firewall ports for each service by using either the vSphere Client or the VMware Host Client.

ESXi includes a firewall that is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the host's security profile. For the list of supported ports and protocols in the ESXi firewall, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/.

The VMware Ports and Protocols Tool lists port information for services that are installed by default. If you install other VIBs on your host, additional services and firewall ports might become available. The information is primarily for services that are visible in the vSphere Client but the VMware Ports and Protocols Tool includes some other ports as well.

Required Free Space for System Logging

If you used Auto Deploy to install your ESXi7.0 host, or if you set up a log directory separate from the default location in a scratch directory on the VMFS volume, you might need to change your current log size and rotation settings to ensure that enough space is available for system logging .

All vSphere components use this infrastructure. The default values for log capacity in this infrastructure vary, depending on the amount of storage available and on how you have configured system logging. Hosts that are deployed with Auto Deploy store logs on a RAM disk, which means that the amount of space available for logs is small.

If your host is deployed with Auto Deploy, reconfigure your log storage in one of the following ways:

- Redirect logs over the network to a remote collector.
- Redirect logs to a NAS or NFS store.

If you redirect logs to non-default storage, such as a NAS or NFS store, you might also want to reconfigure log sizing and rotations for hosts that are installed to disk.

You do not need to reconfigure log storage for ESXi hosts that use the default configuration, which stores logs in a scratch directory on the VMFS volume. For these hosts, ESXi7.0 configures logs to best suit your installation, and provides enough space to accommodate log messages.

Table 31: Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

VMware Host Client System Requirements

Make sure that your browser supports the VMware Host Client.

The following guest operating systems and Web browser versions are supported for the VMware Host Client.

Supported Browsers	Mac OS	Windows 32-bit and 64-bit	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	N/A
Safari	9.0+	N/A	N/A

ESXi Passwords and Account Lockout

For ESXi hosts, you must use a password with predefined requirements. You can change the required length and character class requirement or allow pass phrases using the Security.PasswordQualityControl advanced option. You can also set the number of passwords to remember for each user using the Security.PasswordHistory advanced option.

Note: The default requirements for ESXi passwords can change from one release to the next. You can check and change the default password restrictions by using the Security.PasswordQualityControl advanced option.

ESXi Passwords

ESXi enforces password requirements for access from the Direct Console User Interface, the ESXi Shell, SSH, or the VMware Host Client.

- By default, you must include a mix of at least three from the following four character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash when you create a password.
- By default, password length is at least 7 characters and less than 40.
- Passwords must not contain a dictionary word or part of a dictionary word.
- Passwords must not contain the user name or parts of the user name.

Note: An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used. A dictionary word used inside a password reduces the overall password strength.

Example ESXi Passwords

The following password candidates illustrate potential passwords if the option is set as follows.

```
retry=3 min=disabled,disabled,disabled,7,7
```

With this setting, a user is prompted up to three times (retry=3) for a new password that is not sufficiently strong or if the password was not entered correctly twice. Passwords with one or two character classes and pass phrases are not allowed, because the first three items are disabled. Passwords from three- and four-character classes require seven characters. See the `pam_passwdqc` man page for details on other options, such as max, passphrase, and so on.

With these settings, the following passwords are allowed.

- xQaTEhb!: Contains eight characters from three character classes.
- xQaT3#A: Contains seven characters from four character classes.

The following password candidates do not meet requirements.

- Xqat3hi: Begins with an uppercase character, reducing the effective number of character classes to two. The minimum number of required character classes is three.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. The minimum number of required character classes is three.

ESXi Pass Phrase

Instead of a password, you can also use a pass phrase. However, pass phrases are disabled by default. You can change the default setting and other settings by using the Security.PasswordQualityControl advanced option from the vSphere Client.

For example, you can change the option to the following.

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows pass phrases of at least 16 characters and at least three words.

For legacy hosts, changing the `/etc/pam.d/passwd` file is still supported, but changing the file is deprecated for future releases. Use the Security.PasswordQualityControl advanced option instead.

Changing Default Password Restrictions

You can change the default restriction on passwords or pass phrases by using the Security.PasswordQualityControl advanced option for your ESXi host. See *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

You can change the default, for example, to require a minimum of 15 characters and a minimum number of four words (passphrase=4), as follows:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

See the man page for `pam_passwdqc` for details.

Note: Not all possible combinations of password options have been tested. Perform testing after you change the default password settings.

This example sets the password complexity requirement to require eight characters from four character classes that enforce a significant password difference, a remembered history of five passwords, and a 90 day rotation policy:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Set the Security.PasswordHistory option to 5 and the Security.PasswordMaxDays option to 90.

ESXi Account Lockout Behavior

Account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of five failed attempts is allowed before the account is locked. The account is unlocked after 15 minutes by default.

Configuring Login Behavior

You can configure the login behavior for your ESXi host with the following advanced options:

- Security.AccountLockFailures. Maximum number of failed login attempts before a user's account is locked. Zero deactivates account locking.
- Security.AccountUnlockTime. Number of seconds that a user is locked out.
- Security.PasswordHistory. Number of passwords to remember for each user. Zero deactivates password history.

See the *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

Before Upgrading ESXi Hosts

For a successful upgrade of your ESXi hosts, understand and prepare for the changes that are involved.

For a successful upgrade, follow these best practices:

1. Make sure that you understand the upgrade process, the effect of that process on your existing deployment, and the preparation required for the upgrade.
   - If your vSphere system includes VMware solutions or plug-ins, make sure they are compatible with the vCenter Server version that you are upgrading to. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
   - Read Overview of the ESXi Host Upgrade Process to understand the upgrade scenarios that are supported, and the options and tools that are available to perform the upgrade.
   - Read the VMware vSphere Release Notes for known installation issues.
2. Prepare the system for the upgrade.
   - Make sure that the current version is supported for the upgrade. See Overview of the ESXi Host Upgrade Process.
   - Make sure that the system hardware complies with requirements. See ESXi Requirements and VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php. Check for system compatibility, I/O compatibility with network and host bus adapter (HBA) cards, storage compatibility, and backup software compatibility.
   - Make sure that sufficient disk space is available on the host for the upgrade.
   - If a SAN is connected to the host, detach the Fibre Channel system before continuing with the upgrade. Do not deactivate HBA cards in the BIOS.
3. Back up the host before performing an upgrade. If the upgrade fails, you can restore the host.

4. If you are using Auto Deploy to provision hosts, the user who is running the process must have local administrator privileges on the ESXi host that is being provisioned. By default the installation process has these privileges and certificate provisioning happens as expected. However, if you are using another method than the installer, you must run it as a user who has the local administrator privileges.
5. Depending on the upgrade option you choose, you might need to migrate or power off all virtual machines on the host. See the instructions for your upgrade method.
   – For an interactive upgrade from CD, DVD, or USB drive: see Upgrade Hosts Interactively.
   – For a scripted upgrade: see Installing or Upgrading Hosts by Using a Script.
   – For vSphere Auto Deploy: see Using vSphere Auto Deploy to Reprovision Hosts. If the ESXi 6.5x or 6.7.x host was deployed by using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with a 7.0 image.
   – For the `esxcli` command method: see Upgrading Hosts by Using ESXCLI Commands .
6. Plan for the tasks that must be performed after the ESXi host upgrade:
   – Test the system to ensure that the upgrade completed successfully.
   – Apply a host's licenses. See Licensing ESXi Hosts After Upgrade.
   – Consider setting up a syslog server for remote logging, to ensure sufficient disk storage for log files. Setting up logging on a remote host is especially important for hosts with limited local storage. You can optionally install VMware vCenter Log Insight, which provides log aggregation and analytics. See Required Free Space for System Logging.
7. If the upgrade was unsuccessful and you backed up the host, you can restore the host.

Upgrading Hosts That Have Third-Party Custom VIBs

A host can have custom vSphere Installation Bundles (VIBs) installed, for example, third-party drivers or management agents.

When you upgrade an ESXi host to 7.0, all supported custom VIBs are migrated, regardless of whether the VIBs are included in the installer ISO. If the host or the installer ISO image contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the VIB that created the conflict. To upgrade the host, take one of the following actions:

- Remove the VIB that created the conflict from the ESXi host and retry the upgrade. You can remove a VIB from the host by using `esxcli` commands. For more information, see Remove VIBs from a Host.
- Use the vSphere ESXi Image Builder CLI to create a custom installer ISO image that resolves the conflict. For more information about vSphere ESXi Image Builder CLI, see the *vCenter Server Installation and Setup* documentation.

Upgrading ESXi Hosts in an Environment With VMware NSX

In a VMware NSX setup, before an upgrade to ESXi 7.0 and later, make sure that the NSX kernel module is part of the image or upgrade baseline.

If your vSphere system includes VMware NSX, before you start an upgrade of your ESXi hosts, you must ensure that the NSX kernel module is part of the desired software specification or baseline that you use for the upgrade. When you upgrade an ESXi host to 7.0 or later, all supported custom VIBs are migrated, regardless of whether the VIBs are included in the installer ISO. However, the NSX kernel module is not automatically migrated to the installer ISO image. Before you proceed to the upgrade operation, see the knowledge base articles 325109, 78679, and 312013.

Media Options for Booting the ESXi Installer

The ESXi installer must be accessible to the system on which you are installing ESXi.

The following boot media are supported for the ESXi installer:

- Boot from a CD/DVD. See Download and Burn the ESXi Installer ISO Image to a CD or DVD.

- Boot from a USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade.
- Boot from a network. See Network Booting the ESXi Installer.
- Boot from a remote location using a remote management application. See Using Remote Management Applications.

Download and Burn the ESXi Installer ISO Image to a CD or DVD

If you do not have an ESXi installation CD/DVD, you can create one.

You can also create an installer ISO image that includes a custom installation script. See Create an Installer ISO Image with a Custom Installation or Upgrade Script.

1. Follow the procedure Download the ESXi Installer.
2. Burn the ISO image to a CD or DVD.

Format a USB Flash Drive to Boot the ESXi Installation or Upgrade

You can format a USB flash drive to boot the ESXi installation or upgrade.

- Linux machine with superuser access to it
- USB flash drive that can be detected by the Linux machine
- The ESXi ISO image, `VMware-VMvisor-Installer-`*`version_number-build_number`*`.x86_64.iso`, which includes the `isolinux.cfg` file

The instructions in this procedure assume that the USB flash drive is detected as `/dev/sdb`.

Note: The `ks.cfg` file that contains the installation script cannot be located on the same USB flash drive that you are using to boot the installation or upgrade. The kickstart file does not have any dependency on BIOS or UEFI boot.

1. Boot Linux, log in, and enter superuser mode by using a `su` or `sudo root` command.
2. If your USB flash drive is not detected as `/dev/sdb`, or you are not sure how your USB flash drive is detected, determine how it is detected.
   a) Plug in your USB flash drive.
   b) At the command line, run the command for displaying the current log messages.

      ```
      tail -f /var/log/messages
      ```

      You see several messages that identify the USB flash drive in a format similar to the following message.

      ```
      Oct 25 13:25:23 ubuntu kernel: [  712.447080] sd 3:0:0:0: [sdb] Attached SCSI
       removable disk
      ```

      In this example, `sdb` identifies the USB device. If your device is identified differently, use that identification in place of *`sdb`*.
3. Overwrite the entire USB drive with the ISO image. This overwrites the partition table and any previous content on the USB drive.

   ```
   dd bs=10M if=VMware-VMvisor-Installer-version_number-build_number.x86_64.iso of=/dev/
   sdb
   ```
4. Eject the USB drive.

   ```
   eject /dev/sdb
   ```

You can use the USB flash drive to boot the ESXi installer.

Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script

You can use a USB flash drive to store the ESXi installation script or upgrade script that is used during scripted installation or upgrade of ESXi.

- Linux machine
- ESXi installation or upgrade script, the `ks.cfg` kickstart file
- USB flash drive

When multiple USB flash drives are present on the installation machine, the installation software searches for the installation or upgrade script on all attached USB flash drives.

The instructions in this procedure assume that the USB flash drive is detected as `/dev/sdb`.

Note: Do not store the `ks` file containing the installation or upgrade script on the same USB flash drive that you are using to boot the installation or upgrade.

1. Attach the USB flash drive to a Linux machine that has access to the installation or upgrade script.
2. Create a partition table.

   ```
   /sbin/fdisk /dev/sdb
   ```

   a) Type `d` to delete partitions until they are all deleted.
   b) Type `n` to create primary partition 1 that extends over the entire disk.
   c) Type `t` to set the type to an appropriate setting for the FAT32 file system, such as `c`.
   d) Type `p` to print the partition table.

   The result should be similar to the following text:

   ```
   Disk /dev/sdb: 2004 MB, 2004877312 bytes
   255 heads, 63 sectors/track, 243 cylinders
   Units = cylinders of 16065 * 512 = 8225280 bytes
      Device Boot      Start         End      Blocks   Id  System
   /dev/sdb1               1         243      1951866  c   W95 FAT32 (LBA)
   ```

   e) Type `w` to write the partition table and quit.
3. Format the USB flash drive with the FAT32 file system.

   ```
   /sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
   ```
4. Create a destination directory and mount the USB flash drive to it.

   ```
   mkdir -p /usbdisk
   mount /dev/sdb1 /usbdisk
   ```
5. Copy the ESXi installation script to the USB flash drive.

   ```
   cp ks.cfg /usbdisk
   ```
6. Unmount the USB flash drive.

   ```
   umount /usbdisk
   ```

The USB flash drive contains the installation or upgrade script for ESXi.

When you boot the ESXi installer, point to the location of the USB flash drive for the installation or upgrade script. See Enter Boot Options to Run an Installation or Upgrade Script and PXELINUX Configuration Files.

Create an Installer ISO Image with a Custom Installation or Upgrade Script

You can customize the standard ESXi installer ISO image with your own installation or upgrade script. This customization enables you to perform a scripted, unattended installation or upgrade when you boot the resulting installer ISO image.

- Linux machine
- The ESXi ISO image `VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso`,where *x.x.x* is the version of ESXi you are installing, and *XXXXXX* is the build number of the installer ISO image
- Your custom installation or upgrade script, the `KS_CUST.CFG` kickstart file

See also About Installation and Upgrade Scripts and About the boot.cfg File .

1. Download the ESXi ISO image from the Broadcom Support Portal.
2. Mount the ISO image in a folder:

   ```
   mount -o loop VMware-VMvisor-Installer-x.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount
   ```

   `XXXXXX` is the ESXi build number for the version that you are installing or upgrading to.
3. Copy the contents of `esxi_cdrom` to another folder:

   ```
   cp -r /esxi_cdrom_mount/* /esxi_cdrom
   ```
4. Copy the kickstart file to `/esxi_cdrom`.

   ```
   cp KS_CUST.CFG /esxi_cdrom
   ```
5. Modify the `boot.cfg` file in both `/esxi_cdrom/efi/boot/boot.cfg` (for UEFI boot) and `/esxi_cdrom/boot.cfg` (for legacy BIOS boot) to specify the location of the installation or upgrade script by using the `kernelopt` option.

   You must use uppercase characters to provide the path of the script, for example,

   ```
   kernelopt=runweasel ks=cdrom:/KS_CUST.CFG
   ```

   The installation or upgrade becomes completely automatic, without the need to specify the kickstart file during the installation or upgrade.
6. Recreate the ISO image using the `mkisofs` or the `genisoimage` command.

Command	Syntax
mkisofs	`mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -eltorito-platform efi -b EFIBOOT.IMG -no-emul-boot /esxi_cdrom`
genisoimage	`genisoimage -relaxed-filenames -J -R -o custom_esxi.iso -b ISOLINUX.BIN -c BOOT.CAT -no-emul-boot -boot-load-size 4 -boot-info-table -eltorito-alt-boot -e EFIBOOT.IMG -no-emul-boot /esxi_cdrom`

   You can use this ISO installer image for regular boot or UEFI secure boot. However, the vSphere Lifecycle Manager cannot verify the checksum of such an ISO image and you cannot use it for upgrades by using vSphere Lifecycle Manager workflows.

The ISO image includes your custom installation or upgrade script.

Install ESXi from the ISO image.

Network Booting the ESXi Installer

You can use preboot execution environment (PXE) to boot an ESXi host from a network device, if your host uses legacy BIOS or UEFI.

Alternatively, if your ESXi host supports native UEFI HTTP, you can use hypertext transfer protocol (HTTP) to boot the host from a network device. ESXi is distributed in an ISO format that is used to install to flash memory or to a local hard drive. You can extract the files and boot them over a network interface.

PXE uses Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP) to boot an operating system over a network.

PXE booting requires some network infrastructure and a machine with a PXE-capable network adapter. Most machines that can run ESXi have network adapters that can PXE boot.

Native UEFI HTTP uses DHCP and HTTP to boot over a network. UEFI HTTP boot requires a network infrastructure, UEFI firmware version on the ESXi host that includes HTTP boot feature, and a network adapter that supports UEFI networking.

Booting by using HTTP is faster and more reliable than using TFTP. This is due to the capabilities of the TCP protocol that underlies the HTTP, such as built-in streaming and lost packet recovery. If your ESXi hosts do not support native UEFI HTTP, you can use iPXE HTTP for the boot process.

Note: Network booting with legacy BIOS firmware is possible only over IPv4. Network booting with UEFI BIOS firmware is possible over IPv4 or IPv6.

Installing and Booting ESXi with Software FCoE

You can install and boot ESXi from an FCoE LUN using VMware software FCoE adapters and network adapters with FCoE offload capabilities. Your host does not require a dedicated FCoE HBA.

Note: Starting from vSphere 7.0, VMware deprecates software FCoE adapters in production environments.

The boot LUN must not be shared between hosts and must have a size of minimum of 32 GB. See the *vSphere Storage* documentation for information about installing and booting ESXi with software FCoE.

Using Remote Management Applications

Remote management applications allow you to install ESXi on servers that are in remote locations.

Remote management applications supported for installation include HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II). For a list of currently supported server models and remote management firmware versions, see Supported Remote Management Server Models and Firmware Versions. For support on remote management applications, contact the vendor.

You can use remote management applications to do both interactive and scripted installations of ESXi remotely.

If you use remote management applications to install ESXi, the virtual CD might encounter corruption problems with systems or networks operating at peak capacity. If a remote installation from an ISO image fails, complete the installation from the physical CD media.

Download the ESXi Installer

You can obtain the ESXi installer software either from an OEM or from the Broadcom Support Portal.

Register on the Broadcom Support Portal. For more information, see Register for an account on the Broadcom Support Portal and Communities.

For product download instructions, see Download Broadcom products and software.

For download of offline bundle ZIP files for ESXi patches and updates, see Downloading Broadcom PTF files and solutions.

For more information, see VMware to Broadcom Support Frequently Asked Questions.

Storage Device Names and Identifiers

In the ESXi environment, each storage device is identified by several names.

Device Identifiers

Depending on the type of storage, the ESXi host uses different algorithms and conventions to generate an identifier for each storage device.

Storage-provided identifiers

The ESXi host queries a target storage device for the device name. From the returned metadata, the host extracts or generates a unique identifier for the device. The identifier is based on specific storage standards, is unique and persistent across all hosts, and has one of the following formats:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Path-based identifier

When the device does not provide an identifier, the host generates an mpx.*path* name, where *path* represents the first path to the device, for example, `mpx.vmhba1:C0:T1:L3`. This identifier can be used in the same way as the storage-provided identifies.

The mpx.*path* identifier is created for local devices on the assumption that their path names are unique. However, this identifier is not unique or persistent, and can change after every system restart.

Typically, the path to the device has the following format:

vmhba*Adapter*:C*Channel*:T*Target*:L*LUN*

- vmhba*Adapter* is the name of the storage adapter. The name refers to the physical adapter on the host, not to the SCSI controller used by the virtual machines.
- C*Channel* is the storage channel number.
  Software iSCSI adapters and dependent hardware adapters use the channel number to show multiple paths to the same target.
- T*Target* is the target number. Target numbering is determined by the host and might change when the mappings of targets visible to the host change. Targets that are shared by different hosts might not have the same target number.
- L*LUN* is the LUN number that shows the position of the LUN within the target. The LUN number is provided by the storage system. If a target has only one LUN, the LUN number is always zero (0).

For example, `vmhba1:C0:T3:L1` represents LUN1 on target 3 accessed through the storage adapter vmhba1 and channel 0.

Legacy identifier

In addition to the device-provided identifiers or mpx.*path* identifiers, ESXi generates an alternative legacy name for each device. The identifier has the following format:

vml.*number*

The legacy identifier includes a series of digits that are unique to the device. The identifier can be derived in part from the metadata obtained through the SCSI INQUIRY command. For nonlocal devices that do not provide SCSI INQUIRY identifiers,

the vml.*number* identifier is used as the only available unique identifier.

Displaying Device Names in the vSphere CLI

You can use the `esxcli storage core device list` command to display all device names in the vSphere CLI. The output is similar to the following example:

```
# esxcli storage core device list
naa.XXX
   Display Name: DGC Fibre Channel Disk(naa.XXX)
   ...
   Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

Upgrade Hosts Interactively

To upgrade ESXi 6.5 hosts or ESXi6.7 hosts to ESXi7.0, you can boot the ESXi installer from a CD, DVD, or USB flash drive.

- Verify that the ESXi installer ISO in one of the following locations.
  - On CD or DVD. If you do not have the installation CD or DVD, you can create one. See Download and Burn the ESXi Installer ISO Image to a CD or DVD
  - On a USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade

  Note: You can also use PXE to boot the ESXi installer to run an interactive installation or a scripted installation. See Overview of the Network Boot Installation Process.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- ESXi Embedded must not be on the host. ESXi Installable and ESXi Embedded cannot exist on the same host.
- If you are upgrading an ESXi host, supported custom VIBs that are not included in the ESXi installer ISO are migrated. See Upgrading Hosts That Have Third-Party Custom VIBs
- See your hardware vendor documentation for information about changing the boot order.

Before upgrading, consider disconnecting the network storage. This action decreases the time it takes the installer to search for available disk drives. When you disconnect network storage, any files on the disconnected disks are unavailable at installation. Do not disconnect a LUN that contains an existing ESXi installation.

1. Insert the ESXi installer CD or DVD in the CD-ROM or DVD-ROM drive, or attach the Installer USB flash drive and restart the machine.
2. Set the BIOS to boot from the CD-ROM device or the USB flash drive.
3. In the Select a Disk panel, select the drive on which to install or upgrade ESXi and press Enter.

   Press F1 for information about the selected disk.

   Note: Do not rely on the disk order in the list to select a disk. The disk order is determined by the BIOS. On systems where drives are continuously being added and removed, they might be out of order.
4. Upgrade or install ESXi if the installer finds an existing ESXi installation and VMFS datastore.

   If an existing VMFS datastore cannot be preserved, you can choose only to install ESXi and overwrite the existing VMFS datastore, or to cancel the installation. If you choose to overwrite the existing VMFS datastore, back up the datastore first.

5. Press F11 to confirm and start the upgrade.
6. Remove the installation CD or DVD or USB flash drive when the upgrade is complete.
7. Press Enter to reboot the host.
8. Set the first boot device to be the drive which you selected previously when you upgraded ESXi.

Installing or Upgrading Hosts by Using a Script

You can quickly deploy hosts by using scripted, unattended installations or upgrades.

Scripted installations or upgrades provide an efficient way to deploy multiple hosts. The installation or upgrade script contains the installation settings for . You can apply the script to all hosts that you want to have a similar configuration.

For a scripted installation or upgrade, you must use the supported commands to create a script. You can edit the script to change settings that are unique for each host.

The installation or upgrade script can reside in one of the following locations:

- FTP server
- HTTP/HTTPS server
- NFS server
- USB flash drive
- CD-ROM drive

Enter Boot Options to Run an Installation or Upgrade Script

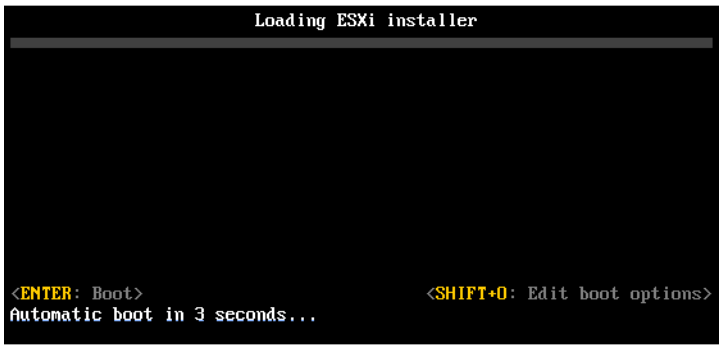
You can start an installation or upgrade script by typing boot options at the ESXi installer boot command line.

At boot time you might need to specify options to access the kickstart file. You can enter boot options by pressing Shift+O in the boot loader. For a PXE boot installation, you can pass options through the `kernelopts` line of the `boot.cfg` file. See About the boot.cfg File and Network Booting the ESXi Installer.

To specify the location of the installation script, set the `ks=`*`filepath`* option, where *`filepath`* indicates the location of your kickstart file. Otherwise, a scripted installation or upgrade cannot start. If `ks=`*`filepath`* is omitted, the text installer is run.

Supported boot options are listed in Boot Options .

1. Start the host.
2. When the ESXi installer window appears, press Shift+O to edit boot options.



3. At the `runweasel` command prompt, type `ks=`*`location of installation script plus boot command-line options`*.

   Boot Option

   You type the following boot options:

   ```
   ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000 net-
   mask=255.255.255.0 gateway=00.00.00.000
   ```

Boot Options

When you perform a scripted installation, you might need to specify options at boot time to access the kickstart file.

Supported Boot Options

Table 32: Boot Options for ESXi Installation

Boot Option	Description
`BOOTIF=`*`hwtype-MAC address`*	Similar to the `netdevice` option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the `syslinux.org` site.
`gateway=`*`ip address`*	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
`ip=`*`ip address`*	Sets up a static IP address to be used for downloading the installation script and the installation media. Note: the PXELINUX format for this option is also supported. See the IPAPPEND option under SYSLINUX at the `syslinux.org` site.
`ks=cdrom:/`*`path`*	Performs a scripted installation with the script at *`path`*, which resides on the CD in the CD-ROM drive. Each CDROM is mounted and checked until the file that matches the path is found. **Important:** If you have created an installer ISO image with a custom installation or upgrade script, you must use uppercase characters to provide the path of the script, for example, `ks=cdrom:/KS_CUST.CFG`.
`ks=file://`*`path`*	Performs a scripted installation with the script at *`path`*.
`ks=`*`protocol`*`://`*`serverpath`*	Performs a scripted installation with a script located on the network at the given URL. *`protocol`* can be `http`, `https`, `ftp`, or `nfs`. An example using NFS protocol is `ks=nfs://`*`host/porturl-path`*. The format of an NFS URL is specified in RFC 2224.
`ks=usb`	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named `ks.cfg`. The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the `ks.cfg` file is found. Only FAT16 and FAT32 file systems are supported.
`ks=usb:/`*`path`*	Performs a scripted installation with the script file at the specified path, which resides on USB.

Boot Option	Description
`ksdevice=device`	Tries to use a network adapter *`device`* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`nameserver=ip address`	Specifies a domain name server to be used for downloading the installation script and installation media.
`netdevice=device`	Tries to use a network adapter *`device`* when looking for an installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnicNN name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
`netmask=subnet mask`	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
`vlanid=vlanid`	Configure the network card to be on the specified VLAN.
`systemMediaSize=small`	Limits the size of system storage partitions on the boot media. The selected value must fit the purpose of your system. You can select from the following values: • *`min`* (32 GB, for single disk or embedded servers) • *`small`* (64 GB, for servers with at least 512 GB RAM) • *`default`* (128 GB) • *`max`* (consume all available space, for multi-terabyte servers)

For more information on ESXi booting options post installation, see VMware knowledge base article 77009.

About Installation and Upgrade Scripts

The installation/upgrade script is a text file, for example `ks.cfg`, that contains supported commands.

The command section of the script contains the ESXi installation options. This section is required and must appear first in the script.

Locations Supported for Installation or Upgrade Scripts

In scripted installations and upgrades, the ESXi installer can access the installation or upgrade script, also called the kickstart file, from several locations.

The following locations are supported for the installation or upgrade script:

- CD/DVD. See Create an Installer ISO Image with a Custom Installation or Upgrade Script.
- USB Flash drive. See Create a USB Flash Drive to Store the ESXi Installation Script or Upgrade Script.
- A network location accessible through the following protocols: NFS, HTTP, HTTPS, FTP

Path to the Installation or Upgrade Script

You can specify the path to an installation or upgrade script.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` is the path to the ESXi installation script, where*XXX.XXX.XXX.XXX*is the IP address of the machine where the script resides. See About Installation and Upgrade Scripts.

To start an installation script from an interactive installation, you enter the ks= option manually. See Enter Boot Options to Run an Installation or Upgrade Script.

Installation and Upgrade Script Commands

To modify the default installation or upgrade script or to create your own script, use supported commands. Use supported commands in the installation script, which you specify with a boot command when you boot the installer.

To determine which disk to install or upgrade ESXi on, the installation script requires one of the following commands: `install`, `upgrade`, or `installorupgrade`. The `install` command creates the default partitions, including a VMFS datastore that occupies all available space after the other partitions are created.

accepteula or vmaccepteula (Required)

Accepts the ESXi license agreement.

clearpart (Optional)

Clears any existing partitions on the disk. Requires the `install` command to be specified. Carefully edit the `clearpart` command in your existing scripts.

--drives=

Remove partitions on the specified drives.

--alldrives

Ignores the `--drives=` requirement and allows clearing of partitions on every drive.

--ignoredrives=

Removes partitions on all drives except those specified. Required unless the `--drives=` or `--alldrives` flag is specified.

--overwritevmfs

Allows overwriting of VMFS partitions on the specified drives. By default, overwriting VMFS partitions is not allowed.

--firstdisk=
disk-type1
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESXi installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

dryrun (Optional)

Parses and checks the installation script. Does not perform the installation.

install

Specifies that this is a fresh installation. Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*`diskname`* , the *`diskname`* can be a disk name or a full disk filesystem path in ESXi, for example:

- Disk name: `--disk=naa.6d09466044143600247aee55ca2a6405` or
- Device path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

For accepted disk name formats, see Disk Device Names.

--firstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

--ignoressd

Excludes solid-state disks from eligibility for partitioning. This option can be used with the `install` command and the --firstdisk option. This option takes precedence over the --firstdisk option. This option is invalid with the --drive or --disk options and with the `upgrade` and `installorupgrade` commands. See the *vSphere Storage* documentation for more information about preventing SSD formatting during auto-partitioning.

--overwritevsan

You must use the --overwritevsan option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a vSAN disk group. If you use this option and no vSAN partition is on the selected disk, the installation fails. When you install ESXi on a disk that is in vSAN disk group, the result depends on the disk that you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group is wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD is wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD is wiped.

For more information about managing vSAN disk groups, see the *vSphere Storage* documentation.

--overwritevmfs

Required to overwrite an existing VMFS datastore on the disk before installation.

--preservevmfs

Preserves an existing VMFS datastore on the disk during installation.

--novmfsondisk

Prevents a VMFS partition from being created on this disk. Must be used with --overwritevmfs if a VMFS partition exists on the disk.

installorupgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*`diskname`* , the *`diskname`* can be a disk name or a full disk filesystem path in ESXi, for example:

- Disk name: `--disk=naa.6d09466044143600247aee55ca2a6405` or
- Device path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

For accepted disk name formats, see Disk Device Names.

--firstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

--overwritevsan

You must use the --overwritevsan option when you install ESXi on a disk, either SSD or HDD (magnetic), that is in a vSAN disk group. If you use this option and no vSAN partition is on the selected disk, the installation fails. When you install ESXi on a disk that is in a vSAN disk group, the result depends on the disk that you select:

- If you select an SSD, the SSD and all underlying HDDs in the same disk group is wiped.
- If you select an HDD, and the disk group size is greater than two, only the selected HDD is wiped.
- If you select an HDD disk, and the disk group size is two or less, the SSD and the selected HDD is wiped.

For more information about managing vSAN disk groups, see the *vSphere Storage* documentation.

--overwritevmfs

Install ESXi if a VMFS partition exists on the disk, but no ESX or ESXi installation exists. Unless this option is present, the installer fails if a VMFS partition exists on the disk, but an ESX or ESXi installation is missing.

keyboard (Optional)

Sets the keyboard type for the system.

keyboardType

Specifies the keyboard map for the selected keyboard type. *`keyboardType`* must be one of the following types.

- Belgian

- Brazilian
- Croatian
- Czechoslovakian
- Danish
- Estonian
- Finnish
- French
- German
- Greek
- Icelandic
- Italian
- Japanese
- Latin American
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Swiss French
- Swiss German
- Turkish
- Ukrainian
- United Kingdom
- US Default
- US Dvorak

serialnum or vmserialnum (Optional)

The command is supported in ESXi version 5.1 and later. Configures licensing. If not included, ESXi installs in evaluation mode.

--esx=<license-key>

Specifies the vSphere license key to use. The format is 5 five-character groups (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (Optional)

Specifies a network address for the system.

--bootproto=[dhcp|static]

Specifies whether to obtain the network settings from DHCP or set them manually.

--device=

Specifies either the MAC address of the network card or the device name, in the form `vmnicNN` , as in `vmnic0` . This option refers to the uplink device for the virtual switch.

--ip=

Sets an IP address for the machine to be installed, in the form `xxx.xxx.xxx.xxx` . Required with the --bootproto=static option and ignored otherwise.

--gateway=

Designates the default gateway as an IP address, in the form `xxx.xxx.xxx.xxx` . Used with the --bootproto=static option.

--nameserver=

Designates the primary name server as an IP address. Used with the `--bootproto=static` option. Omit this option if you do not intend to use DNS.

The `--nameserver` option can accept two IP addresses. For example: `--nameserver="10.126.87.104[,10.126.87.120]"`

--netmask=

Specifies the subnet mask for the installed system, in the form `255.xxx.xxx.xxx` . Used with the `--bootproto=static` option.

--hostname=

Specifies the host name for the installed system.

--vlanid= ***vlanid***

Specifies which VLAN the system is on. Used with either the --bootproto=dhcp or `--bootproto=static` option. Set to an integer from 1 to 4096.

--addvmportgroup=(0|1)

Specifies whether to add the VM Network port group, which is used by virtual machines. The default value is 1.

paranoid (Optional)

Causes warning messages to interrupt the installation. If you omit this command, warning messages are logged.

part or partition (Optional)

Creates an extra VMFS datastore on the system. Only one datastore per disk can be created. Cannot be used on the same disk as the `install` command. Only one partition can be specified per disk and it can only be a VMFS partition.

datastore name

Specifies where the partition is to be mounted.

--ondisk= or --ondrive=

Specifies the disk or drive where the partition is created.

--onfirstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --onfirstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

reboot (Optional)

Reboots the machine after the scripted installation is complete.

<--noeject>

The CD is not ejected after the installation.

rootpw (Required)

Sets the root password for the system.

--iscrypted

Specifies that the password is encrypted.

password

Specifies the password value.

upgrade

Either the `install`, `upgrade`, or `installorupgrade` command is required to determine which disk to install or upgrade ESXi on.

--disk= or --drive=

Specifies the disk to partition. In the command `--disk=`*`diskname`* , the *`diskname`* can be a disk name or a full disk filesystem path in ESXi, for example:

- Disk name: `--disk=naa.6d09466044143600247aee55ca2a6405` or
- Device path: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*

For accepted disk name formats, see Disk Device Names.

--firstdisk=
disk-type1,
[*disk-type2*,...]

Partitions the first eligible disk found. By default, the eligible disks are set to the following order:

1. Locally attached storage (`local`)
2. Network storage (`remote`)
3. USB disks (`usb`)

You can change the order of the disks by using a comma-separated list appended to the argument. If you provide a filter list, the default settings are overridden. You can combine filters to specify a particular disk, including esx for the first disk with ESX installed on it, model and vendor information, or the name of the VMkernel device driver. For example, to prefer a disk with the model name ST3120814A and any disk that uses the mptsas driver rather than a normal local disk, the argument is --firstdisk=ST3120814A,mptsas,local. You can use `localesx` for local storage that contains ESXi image or `remoteesx` for remote storage that contains ESXi image.

%include or include (Optional)

Specifies another installation script to parse. This command is treated similarly to a multiline command, but takes only one argument.

filename

For example: `%include part.cfg`

%pre (Optional)

Specifies a script to run before the kickstart configuration is evaluated. For example, you can use it to generate files for the kickstart file to include.

--interpreter
=[python|busybox]

Specifies an interpreter to use. The default is busybox.

%post (Optional)

Runs the specified script after package installation is complete. If you specify multiple `%post` sections, they run in the order that they appear in the installation script.

--interpreter
=[python|busybox]

Specifies an interpreter to use. The default is busybox.

--timeout=secs

Specifies a timeout for running the script. If the script is not finished when the timeout expires, the script is forcefully stopped.

--ignorefailure
=[true|false]

If true, the installation is considered a success even if the `%post` script stops with an error.

%firstboot

Creates an `init` script that runs only during the first boot. The script has no effect on subsequent boots. If multiple `%firstboot` sections are specified, they run in the order that they appear in the kickstart file.

Note: You cannot check the semantics of `%firstboot` scripts until the system is booting for the first time. A `%firstboot` script might contain potentially catastrophic errors that are not exposed until after the installation is complete.

Important: The `%firstboot` script does not run, if secure boot is enabled on the ESXi host.

--interpreter
=[python|busybox]

Specifies an interpreter to use. The default is busybox.

Note: You cannot check the semantics of the `%firstboot` script until the system boots for the first time. If the script contains errors, they are not exposed until after the installation is complete.

Disk Device Names

The `install`, `upgrade`, and `installorupgrade` installation script commands require the use of disk device names.

Table 33: Disk Device Names

Format	Example	Description
NAA	naa.6d09466044143600247aee55ca2a6405	SCSI INQUIRY identifier
EUI	eui.3966623838646463	SCSI INQUIRY identifier
T10	t10.SanDisk00Cruzer_Blade000000004C5300011711 18101244	SCSI INQUIRY identifier

Format	Example	Description
VML	vml.00025261	Legacy VMkernel identifier
MPX	mpx.vmhba0:C0:T0:L0	Path-based identifier

For more information on storage device names, see *Storage Device Names and Identifiers* in the *vSphere Storage* documentation.

Storage Device Names and Identifiers

In the ESXi environment, each storage device is identified by several names.

Device Identifiers

Depending on the type of storage, the ESXi host uses different algorithms and conventions to generate an identifier for each storage device.

Storage-provided identifiers

The ESXi host queries a target storage device for the device name. From the returned metadata, the host extracts or generates a unique identifier for the device. The identifier is based on specific storage standards, is unique and persistent across all hosts, and has one of the following formats:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Path-based identifier

When the device does not provide an identifier, the host generates an mpx.*path* name, where *path* represents the first path to the device, for example, `mpx.vmhba1:C0:T1:L3`. This identifier can be used in the same way as the storage-provided identifies.

The mpx.*path* identifier is created for local devices on the assumption that their path names are unique. However, this identifier is not unique or persistent, and can change after every system restart.

Typically, the path to the device has the following format:

vmhba*Adapter*:C*Channel*:T*Target*:L*LUN*

- vmhba*Adapter* is the name of the storage adapter. The name refers to the physical adapter on the host, not to the SCSI controller used by the virtual machines.
- C*Channel* is the storage channel number.
  Software iSCSI adapters and dependent hardware adapters use the channel number to show multiple paths to the same target.
- T*Target* is the target number. Target numbering is determined by the host and might change when the mappings of targets visible to the host change. Targets that are shared by different hosts might not have the same target number.
- L*LUN* is the LUN number that shows the position of the LUN within the target. The LUN number is provided by the storage system. If a target has only one LUN, the LUN number is always zero (0).

For example, `vmhba1:C0:T3:L1` represents LUN1 on target 3 accessed through the storage adapter vmhba1 and channel 0.

Legacy identifier

In addition to the device-provided identifiers or mpx.*path* identifiers, ESXi generates an alternative legacy name for each device. The identifier has the following format:

vml.*number*

The legacy identifier includes a series of digits that are unique to the device. The identifier can be derived in part from the metadata obtained through the SCSI INQUIRY command. For nonlocal devices that do not provide SCSI INQUIRY identifiers, the vml.*number* identifier is used as the only available unique identifier.

Displaying Device Names in the vSphere CLI

You can use the `esxcli storage core device list` command to display all device names in the vSphere CLI. The output is similar to the following example:

```
# esxcli storage core device list
naa.XXX
   Display Name: DGC Fibre Channel Disk(naa.XXX)
   ...
   Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

About the boot.cfg File

The boot loader configuration file `boot.cfg` specifies the kernel, the kernel options, and the boot modules that the `mboot.c32` or `mboot.efi` boot loader uses in an ESXi installation.

The `boot.cfg` file is provided in the ESXi installer. You can modify the kernelopt line of the `boot.cfg` file to specify the location of an installation script or to pass other boot options.

The `boot.cfg` file has the following syntax:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
prefix=DIRPATH
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1---FILEPATH2... ---FILEPATHn

# Any other line must remain unchanged.
```

The commands in `boot.cfg` configure the boot loader.

Table 34: Commands in boot.cfg.

Command	Description
`title=`*`STRING`*	Sets the boot loader title to *`STRING`*.
`prefix=`*`STRING`*	(Optional) Adds *`DIRPATH/`* in front of every *`FILEPATH`* in the `kernel=` and `modules=` commands that do not already start with / or with `http://`.
`kernel=`*`FILEPATH`*	Sets the kernel path to *`FILEPATH`*.
`kernelopt=`*`STRING`*	Appends *`STRING`* to the kernel boot options.
`modules=`*`FILEPATH1 --- FILEPATH2... --- FILEPATHn`*	Lists the modules to be loaded, separated by three hyphens (`---`).

See Create an Installer ISO Image with a Custom Installation or Upgrade Script and Network Booting the ESXi Installer.

Install or Upgrade ESXi from a CD or DVD by Using a Script

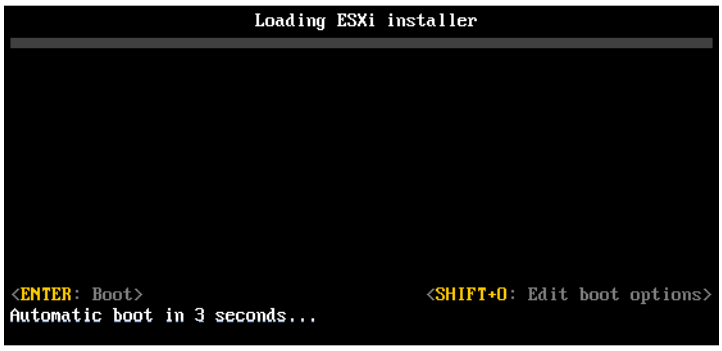
You can install or upgrade ESXi from a CD-ROM or DVD-ROM drive by using a script that specifies the installation or upgrade options.

Before you run the scripted installation or upgrade, verify that the following prerequisites are met:

- The system on which you are installing or upgrading meets the hardware requirements. See ESXi Hardware Requirements.
- You have the ESXi installer ISO on an installation CD or DVD . See Download and Burn the ESXi Installer ISO Image to a CD or DVD.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See About Installation and Upgrade Scripts.
- You have selected a boot command to run the scripted installation or upgrade. See Enter Boot Options to Run an Installation or Upgrade Script. For a complete list of boot commands, see Boot Options .

You can start the installation or upgrade script by entering a boot option when you start the host. You can also create an installer ISO image that includes the installation script. With an installer ISO image, you can perform a scripted, unattended installation when you boot the resulting installer ISO image. See Create an Installer ISO Image with a Custom Installation or Upgrade Script.

1. Boot the ESXi installer from the local CD-ROM or DVD-ROM drive.
2. When the ESXi installer window appears, press Shift+O to edit boot options.



3. Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

   The boot option has the form `ks=` .

4. Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Install or Upgrade ESXi from a USB Stick by Using a Script

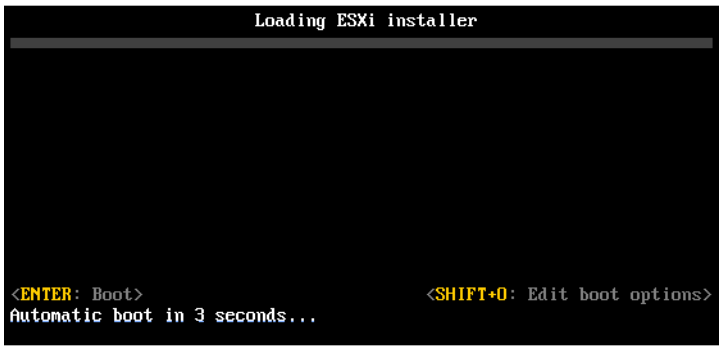
You can install or upgrade ESXi from a USB flash drive by using a script that specifies the installation or upgrade options.

Before running the scripted installation or upgrade, verify that the following prerequisites are met:

- The system that you are installing or upgrading to ESXi meets the hardware requirements for the installation or upgrade. See ESXi Hardware Requirements.
- You have the ESXi installer ISO on a bootable USB flash drive. See Format a USB Flash Drive to Boot the ESXi Installation or Upgrade.
- The default installation or upgrade script (`ks.cfg`) or a custom installation or upgrade script is accessible to the system. See About Installation and Upgrade Scripts.
- You have selected a boot option to run the scripted installation, upgrade, or migration. See Enter Boot Options to Run an Installation or Upgrade Script.

Supported boot options are listed in Boot Options .

1. Boot the ESXi installer from the USB flash drive.
2. When the ESXi installer window appears, press Shift+O to edit boot options.



3. Type a boot option that calls the default installation or upgrade script or an installation or upgrade script file that you created.

   The boot option has the form `ks=` .

4. Press Enter.

The installation, upgrade, or migration runs, using the options that you specified.

Network Boot the ESXi Installer for a Scripted Installation or Upgrade

ESXi7.0 provides many options for booting the installer over a network and using an installation or upgrade script.

- For information about setting up a network infrastructure, see Network Booting the ESXi Installer.
- For information about creating and locating an installation script, see About Installation and Upgrade Scripts.
- For specific procedures to network boot the ESXi installer and use an installation script, see one of the following topics:

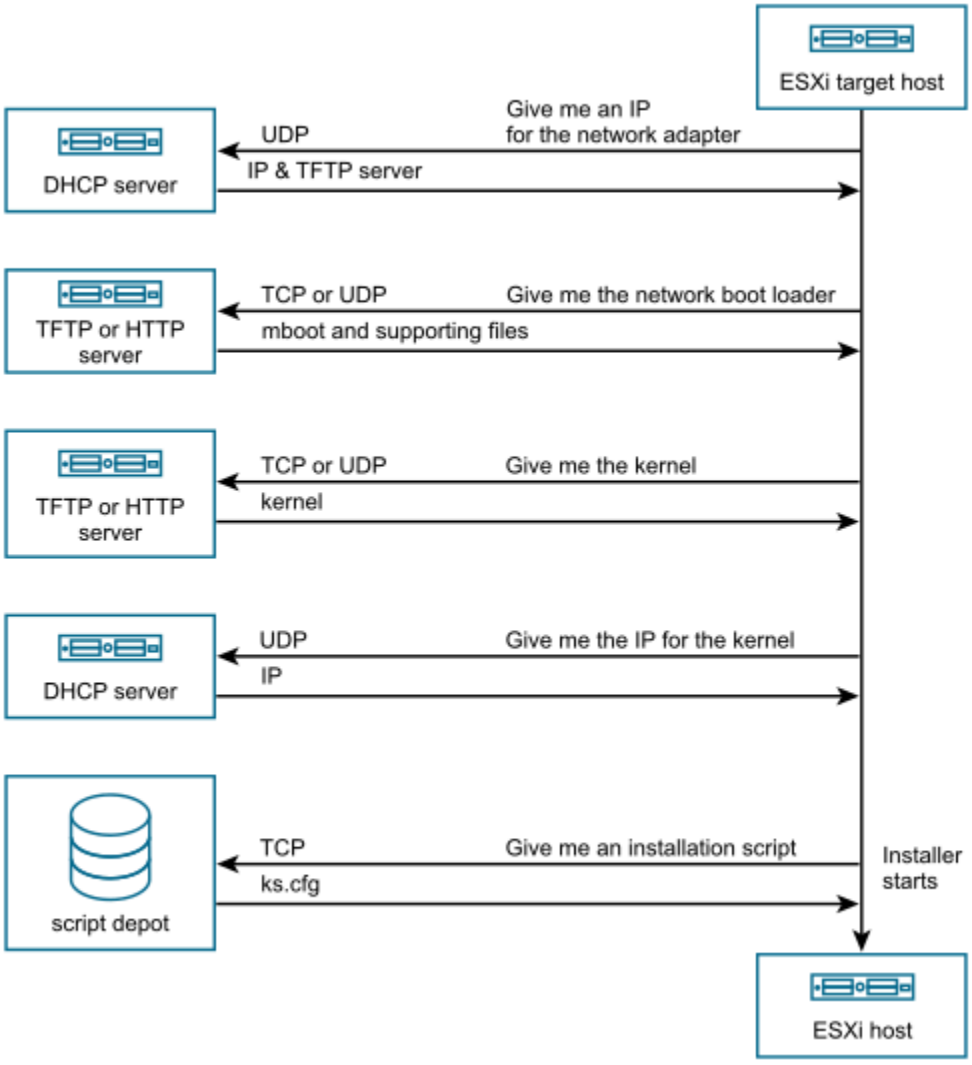
- Boot the ESXi Installer by Using Native UEFI HTTP
- Boot the ESXi Installer by Using iPXE and HTTP
- Boot the ESXi Installer by Using PXE and TFTP

Overview of the Network Boot Installation Process

You can boot an ESXi host from a network interface. The network boot process varies depending on whether the target host is using legacy BIOS or UEFI firmware, and whether the boot process uses PXE TFTP, iPXE HTTP, or UEFI HTTP.

When you boot a target host, it interacts with the different servers in the environment to get a network adapter, boot loader, kernel, IP address for the kernel, and finally an installation script. When all components are in place, installation starts, as shown in the following illustration.

Figure 15: Overview of PXE Boot Installation Process



The interaction between the ESXi host and other servers proceeds as follows:

1. The user boots the target ESXi host.
2. The target ESXi host makes a DHCP request.

3. The DHCP server responds with the IP information, the location of the TFTP or HTTP server, and the filename or URL of the initial network boot loader.
4. The ESXi host contacts the TFTP or HTTP server and requests the filename or URL that the DHCP server specified.
5. The TFTP or HTTP server sends the network boot loader, and the ESXi host runs it. The initial boot loader might load additional boot loader components from the server.
6. The boot loader searches for a configuration file on the TFTP or HTTP server, downloads the kernel and other ESXi components as specified in the configuration file, and boots the kernel on the ESXi host.
7. The installer runs interactively or using a kickstart script, as specified in the configuration file.

Boot the ESXi Installer by Using PXE and TFTP

You can use a TFTP server to PXE boot the ESXi installer. The process differs slightly depending on whether you use UEFI or boot from a legacy BIOS. Because most environments include ESXi hosts that support UEFI boot and hosts that support only legacy BIOS, this topic discusses prerequisites and steps for both types of hosts.

Verify that your environment meets the following prerequisites.

- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.
- Network adapter with PXE support on the target ESXi host.
- DHCP server that you can configure for PXE booting. See Sample DHCP Configurations.
- TFTP server.
- Network security policies to allow TFTP traffic (UDP port 69).
- For legacy BIOS, you can use only IPv4 networking. For UEFI PXE boot, you can use IPv4 or IPv6 networking.
- (Optional) Installation script (kickstart file).
- Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

For legacy BIOS systems, obtain version 3.86 of the SYSLINUX package. For more information, see Network Boot Background Information.

- For legacy BIOS machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `pxelinux.0` initial boot loader for all target machines, but potentially different PXELINUX configuration files depending on the target machine's MAC address.
- For UEFI machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

1. If your ESXi host runs legacy BIOS firmware only, obtain and configure PXELINUX.
   a) Obtain SYSLINUX version 3.86, unpack it, and copy the `pxelinux.0` file to the top-level `/tftpboot` directory on your TFTP server.
   b) Create a PXELINUX configuration file using the following code model.

      `ESXi-7.x.x-XXXXXX` is the name of the TFTP subdirectory that contains the ESXi installer files.

      ```
      DEFAULT install
      NOHALT 1
      LABEL install
        KERNEL ESXi-7.x.x-XXXXXX/mboot.c32
        APPEND -c ESXi-7.x.x-XXXXXX/boot.cfg
        IPAPPEND 2
      ```

c) Save the PXELINUX file in the `/tftpboot/pxelinux.cfg` directory on your TFTP server with a filename that will determine whether all hosts boot this installer by default:

Option	Description
Same installer	Name the file `default` if you want all host to boot this ESXi installer by default.
Different installers	Name the file with the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*) if you want only a specific host to boot with this file, for example, `01-23-45-67-89-0a-bc`.

2. If your ESXi host runs UEFI firmware, copy the `efi/boot/bootx64.efi` file from the ESXi installer ISO image to the `/tftpboot` folder on your TFTP server, and rename the file to `mboot.efi`. For 7.0 Update 3 and later, also copy the `efi/boot/crypto64.efi` file to the `/tftpboot` folder.

   Note: Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

3. Configure the DHCP server.
4. Create a subdirectory of your TFTP server's top-level `/tftpboot` directory and name it after the version of ESXi it will hold, for example, `/tftpboot/ESXi-7.x.x-xxxxx`.
5. Copy the contents of the ESXi installer image to the newly created directory.
6. Modify the `boot.cfg` file
   a) Add the following line:

      ```
      prefix=ESXi-7.x.x-xxxxxx
      ```

      Here, `ESXi-7.x.x-xxxxxx` is the pathname of the installer files relative to the TFTP server's root directory.
   b) If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.
   c) If the `kernelopt=` line contains the string `cdromBoot`, remove the string only.
7. Optional: For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option to the line after the kernel command, to specify the location of the installation script.

   Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory that contains the `ks.cfg` file.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

8. If your ESXi host runs UEFI firmware, specify whether you want all UEFI hosts to boot the same installer.

Option	Description
Same installer	Copy or link the `boot.cfg` file to `/tftpboot/boot.cfg`
Different installers	1. Create a subdirectory of `/tftpboot` named after the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), for example, `01-23-45-67-89-0a-bc`. 2. Place a copy of (or a link to) the host's `boot.cfg` file in that directory, for example, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`.

Boot the ESXi Installer by Using iPXE and HTTP

You can use iPXE to boot the ESXi installer from an HTTP server. The following topic discusses prerequisites and steps for ESXi hosts that support UEFI boot and hosts that support legacy BIOS only.

Verify that your environment has the following components:

- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.
- Network adapter with PXE support on the target ESXi host.
- DHCP server that you can configure for PXE booting. See Sample DHCP Configurations.
- TFTP server.
- Network security policies to allow TFTP traffic (UDP port 69).
- For legacy BIOS, you can use only IPv4 networking. For UEFI PXE boot, you can use IPv4 or IPv6 networking.
- (Optional) Installation script (kickstart file).
- Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

Verify that your environment also meets the following prerequisites required for PXE boot using an HTTP Server:

- Verify that the HTTP server is accessible by your target ESXi hosts.
- If your ESXi host runs legacy BIOS firmware only, obtain version 3.86 of the SYSLINUX package. For more information, see Network Boot Background Information.
- For legacy BIOS machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `pxelinux.0` initial boot loader for all target machines, but potentially different PXELINUX configuration files depending on the target machine's MAC address.
- For UEFI machines, the procedure supports booting multiple different versions of the ESXi installer by using the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

1. Obtain and configure iPXE.
   a) Obtain the iPXE source code.
   b) On the iPXE download page, follow the build instructions, but run one of the following commands.
      - For ESXi hosts that run legacy BIOS firmware only, run `make bin/undionly.kpxe`.
      - For ESXi hosts that run UEFI firmware, run `make bin-x86_64-efi/snponly.efi`.
   c) Copy the `undionly.kpxe` or `snponly.efi` file to the `/tftpboot` directory on your TFTP server.
2. If your ESXi host runs legacy BIOS firmware only, obtain and configure PXELINUX.
   a) Obtain SYSLINUX version 3.86, unpack it, and copy the `pxelinux.0` file to the `/tftpboot` directory on your TFTP server.
   b) Create a PXELINUX configuration file using the following code model.
   `ESXi-7.x.x-XXXXXX` is the name of the TFTP subdirectory that contains the ESXi installer files.

```
DEFAULT install
NOHALT 1
LABEL install
  KERNEL ESXi-7.x.x-XXXXXX/mboot.c32
  APPEND -c ESXi-7.x.x-XXXXXX/boot.cfg
  IPAPPEND 2
```

   c) Save the PXELINUX file in the `/tftpboot/pxelinux.cfg` directory on your TFTP server.
   The filename determines whether all hosts boot this installer by default.

Option	Description
Same installer	Name the file `default` if you want all host to boot this ESXi installer by default.

Option	Description
Different installers	Name the file with the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), if only a specific host must boot this file. For example, `01-23-45-67-89-0a-bc`.

3. If your ESXi host runs UEFI firmware, copy the `efi/boot/bootx64.efi` file from the ESXi installer ISO image to the `/tftpboot` folder on your TFTP server, and rename the file to `mboot.efi`.

   Note: Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

4. Configure the DHCP server.
5. Create a directory on your HTTP server with the same name as the version of ESXi it will hold. For example, `/var/www/html/ESXi-7.x.x-XXXXXX`.
6. Copy the contents of the ESXi installer image to the newly created directory.
7. Modify the `boot.cfg` file
   a) Add the following line:

      ```
      prefix=http://XXX.XXX.XXX.XXX/ESXi-7.x.x-XXXXXX
      ```

      where `http://XXX.XXX.XXX.XXX/ESXi-7.x.x-XXXXXX` is the location of the installer files on the HTTP server.
   b) If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.
   c) If the `kernelopt=` line contains the string `cdromBoot`, remove the string only.
8. Optional: For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option to the line after the kernel command, to specify the location of the installation script.

   Use the following code as a model, where `XXX.XXX.XXX.XXX` is the IP address of the server where the installation script resides, and `esxi_ksFiles` is the directory that contains the `ks.cfg` file.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

9. If your ESXi host runs UEFI firmware, specify whether you want all UEFI hosts to boot the same installer.

Option	Description
Same installer	Copy or link the `boot.cfg` file to `/tftpboot/boot.cfg`
Different installers	1. Create a subdirectory of `/tftpboot` named after the MAC address of the target host machine (01-*mac_address_of_target_ESXi_host*), for example, `01-23-45-67-89-0a-bc`. 2. Place a copy of (or a link to) the host's `boot.cfg` file in that directory, for example, `/tftpboot/01-23-45-67-89-0a-bc/boot.cfg`.

Boot the ESXi Installer by Using Native UEFI HTTP

You can boot the ESXi installer directly from an HTTP server, without additional software to support the process.

Verify that your environment has the following components:

- ESXi host with UEFI firmware that supports the HTTP boot feature.
- ESXi installer ISO image, downloaded from the VMware Web site.
- Target host with a hardware configuration that is supported for your version of ESXi. See the *VMware Compatibility Guide*.

- Network adapter with UEFI networking support on the target ESXi host.
- DHCP server that you can configure for UEFI HTTP booting. See Sample DHCP Configurations
- (Optional) Installation script (kickstart file).
- Use a native VLAN in most cases. If you want to specify the VLAN ID to be used with PXE booting, check that your NIC supports VLAN ID specification.

UEFI HTTP supports booting multiple versions of the ESXi installer. You use the same `mboot.efi` initial boot loader for all target machines, but potentially different `boot.cfg` files depending on the target machine's MAC address.

Note: Do not mix IPv4 or IPv6 networking during the boot process. Use either IPv4 or IPv6 networking.

1. Copy the `efi/boot/bootx64.efi` file from the ESXi installer ISO image to a directory on your HTTP server and rename the file to `mboot.efi`. For example, `http://www.example.com/esxi/mboot.efi`.

   Note: Newer versions of `mboot.efi` can generally boot older versions of ESXi, but older versions of `mboot.efi` might be unable to boot newer versions of ESXi. If you plan to configure different hosts to boot different versions of the ESXi installer, use the `mboot.efi` from the newest version.

2. Configure the DHCP server.
3. Create a directory on your HTTP server with the same name as the version of ESXi it will hold. For example, `http://www.example.com/esxi/ESXi-7.x.x-XXXXXX`.
4. Copy the contents of the ESXi installer image to the newly created directory.
5. Modify the `boot.cfg` file.
   a) Add the following line with the URL of the newly created directory.

      ```
      prefix=http://www.example.com/esxi/ESXi-7.x.x-XXXXXX
      ```

   b) If the filenames in the `kernel=` and `modules=` lines begin with a forward slash (/) character, delete that character.
   c) If the `kernelopt=` line contains the string `cdromBoot`, remove the string only.
6. Optional: For a scripted installation, in the `boot.cfg` file, add the `kernelopt` option to the line after the kernel command, to specify the location of the installation script.

   For example, `kernelopt=ks=http://www.example.com/esxi_ksFiles/ks.cfg`
7. Optional: Starting with ESXi 7.0 Update 2, you can use the virtual machine configuration parameters *`networkBootProtocol`* and *`networkBootUri`* to specify from where a virtual machines can boot. The setting *`networkBootProtocol`* specifies the boot protocol, IPv4 or IPv6. For example, `networkBootProtocol = httpv4` . The setting *`networkBootUri`* specifies the HTTP URL to the ESXi bootloader (bootx64.efi). For example, `networkBootUri = http://192.168.30.6/esxi70uc1/efi/boot/bootx64.efi` .
8. Specify whether you want all UEFI hosts to boot the same installer.

Option	Description
Same installer	Add the `boot.cfg` file to the same directory as `mboot.efi`. For example, `http://www.example.com/esxi/boot.cfg`
Different installers	1. Create a subdirectory of the directory that contains the `mboot.efi` file. Name the directory as the MAC address of the target host machine (01-*`mac_address_of_target_ESXi_host`*), for example, `01-23-45-67-89-0a-bc`. 2. Add the custom `boot.cfg` file in the directory. For example, `http://www.example.com/esxi/01-23-45-67-89-0a-bc/boot.cfg`.

   You can use both installer types. ESXi hosts without custom `boot.cfg` file on your HTTP server, boot from the default `boot.cfg` file.

Network Boot Background Information

Understanding the network boot process can help you during troubleshooting.

TFTP Server

Trivial File Transfer Protocol (TFTP) is similar to the FTP service, and is typically used only for network booting systems or loading firmware on network devices such as routers. TFTP is available on Linux and Windows.

- Most Linux distributions include a copy of the tftp-hpa server. If you require a supported solution, purchase a supported TFTP server from your vendor of choice. You can also acquire a TFTP server from one of the packaged appliances on the VMware Marketplace.
- If your TFTP server runs on a Microsoft Windows host, use tftpd32 version 2.11 or later. See http://tftpd32.jounin.net/.

SYSLINUX and PXELINUX

If you are using PXE in a legacy BIOS environment, you must understand the different boot environments.

- SYSLINUX is an open-source boot environment for machines that run legacy BIOS firmware. The ESXi boot loader for BIOS systems, `mboot.c32`, runs as a SYSLINUX plugin. You can configure SYSLINUX to boot from several types of media, including disk, ISO image, and network. You can find the SYSLINUX package at http://www.kernel.org/pub/linux/utils/boot/syslinux/.
- PXELINUX is a SYSXLINUX configuration for booting from a TFTP server according to the PXE standard. If you use PXELINUX to boot the ESXi installer, the `pxelinux.0` binary file, `mboot.c32`, the configuration file, the kernel, and other files are transferred by TFTP.

Note: VMware builds the `mboot.c32` plugin to work with SYSLINUX version 3.86 and tests PXE booting only with that version. Other versions might be incompatible. *The Open Source Disclosure Package for VMware vSphere Hypervisor* includes bug fixes for SYSLINUX version 3.86.

iPXE

iPXE is open-source software that provides an implementation of HTTP. You can use the software to perform an initial boot. For more information, see https://ipxe.org/.

VMware includes a build of iPXE as part of Auto Deploy. The source tree for this build is available in *The Open Source Disclosure Package for VMware vCenter Server*.

UEFI PXE and UEFI HTTP

Most UEFI firmware natively includes PXE support that allows booting from a TFTP server. The firmware can directly load the ESXi boot loader for UEFI systems, `mboot.efi`. Additional software such as PXELINUX is not required.

Some UEFI firmware support native UEFI HTTP boot. The feature is introduced in version 2.5 of the UEFI specification. The firmware can load the ESXi boot loader from an HTTP server, without additional software, such as iPXE.

Note: Apple Macintosh products do not include PXE boot support. They include support for network booting through an Apple-specific protocol instead.

Alternative Approaches to Network Booting

Alternative approaches to network booting different software on different hosts are also possible, for example:

- Configuring the DHCP server to provide different initial boot loader filenames to different hosts depending on MAC address or other criteria. See your DCHP server's documentation.
- Approaches using iPXE as the initial bootloader with an iPXE configuration file that selects the next bootloader based on the MAC address or other criteria.

PXELINUX Configuration Files

You need a PXELINUX configuration file to boot the ESXi installer on a legacy BIOS system. The configuration file defines the menu displayed to the target ESXi host as it starts.

This section gives general information about PXELINUX configuration files.

For syntax details, see the SYSLINUX website at http://www.syslinux.org/.

Required Files

In the PXE configuration file, you must include paths to the following files:

- `mboot.c32` is the boot loader.
- `boot.cfg` is the boot loader configuration file.

See About the boot.cfg File

Filename for the PXE Configuration File

For the filename of the PXE configuration file, select one of the following options:

- `01-`*`mac_address_of_target_ESXi_host`*. For example, `01-23-45-67-89-0a-bc`
- The target ESXi host IP address in a hexadecimal notation.
- `default`

The initial boot file `pxelinux.0` tries to load a PXE configuration file in the following order:

1. It tries with the MAC address of the target ESXi host, prefixed with its ARP type code, which is 01 for Ethernet.
2. If that attempt fails, it tries with the hexadecimal notation of target ESXi system IP address.
3. Ultimately, it tries to load a file named `default`.

File Location for the PXE Configuration File

Save the file in `/tftpboot/pxelinux.cfg/` on the TFTP server.

For example, you might save the file on the TFTP server at `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6`. The MAC address of the network adapter on the target ESXi host is 00-21-5a-ce-40-f6.

Sample DHCP Configurations

The DHCP server must send the address of the TFTP or HTTP server and the filename of the initial boot loader to the ESXi host.

When the target machine first boots, it broadcasts a packet across the network requesting information to boot itself. The DHCP server responds. The DHCP server must be able to determine whether the target machine is allowed to boot and the location of the initial boot loader binary. For PXE boot, the location is a file on a TFTP server. For UEFI HTTP boot, the location is a URL.

CAUTION: Do not set up a second DHCP server if your network already has one. If multiple DHCP servers respond to DHCP requests, machines can obtain incorrect or conflicting IP addresses, or can fail to receive the proper boot information. Talk to a network administrator before setting up a DHCP server. For support on configuring DHCP, contact your DHCP server vendor.

There are many DHCP servers that you can use. The following examples are for an ISC DHCP server. If you are using a version of DHCP for Microsoft Windows, see the DHCP server documentation to determine how to pass the next-server and filename arguments to the target machine.

Example of Booting Using PXE and TFTP with IPv4

This example shows how to configure an ISC DHCP server to PXE boot ESXi using a TFTP server at IPv4 address xxx.xxx.xxx.xxx.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      filename = "mboot.efi";
   } else {
      filename = "pxelinux.0";
   }
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `pxelinux.0` or `mboot.efi` binary file on the TFTP server.

Example of Booting Using PXE and TFTP with IPv6

This example shows how to configure an ISC DHCPv6 server to PXE boot ESXi using a TFTP server at IPv6 address xxxx:xxxx:xxxx:xxxx::xxxx.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `mboot.efi` binary file on the TFTP server.

Example of Booting Using iPXE and HTTP with IPv4

This example shows how to configure an ISC DHCP server to boot ESXi by loading iPXE from a TFTP server at IPv4 address `xxx.xxx.xxx.xxx`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
```

```
option client-system-arch code 93 = unsigned integer 16;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xxx.xxx;
   if option client-system-arch = 00:07 or option client-system-arch = 00:09 {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load mboot.efi as secondary bootloader
         filename = "mboot.efi";
      } else {
         # Load the snponly.efi configuration of iPXE as initial bootloader
         filename = "snponly.efi";
      }
   } else {
      if exists user-class and option user-class = "iPXE" {
         # Instruct iPXE to load pxelinux as secondary bootloader
         filename = "pxelinux.0";
      } else {
         # Load the undionly configuration of iPXE as initial bootloader
         filename = "undionly.kpxe";
   }
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `undionly.kpxe` or `snponly.efi` binary file on the TFTP server. In the legacy BIOS case, iPXE then asks the DHCP server for the next file to load, and the server returns `pxelinux.0` as the filename. In the UEFI case, iPXE then asks the DHCP server for the next file to load, and this time the server returns `mboot.efi` as the filename. In both cases, iPXE is resident and the system has HTTP capability. As a result, the system can load additional files from an HTTP server.

Example of Booting Using iPXE and HTTP with IPv6

This example shows how to configure an ISC DHCPv6 server to boot ESXi by loading iPXE from a TFTP server at IPv6 address `xxxx:xxxx:xxxx:xxxx::xxxx`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
if exists user-class and option user-class = "iPXE" {
   # Instruct iPXE to load mboot.efi as secondary bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/mboot.efi";
} else {
   # Load the snponly.efi configuration of iPXE as initial bootloader
   option dhcp6.bootfile-url "tftp://[xxxx:xxxx:xxxx:xxxx::xxxx]/snponly.efi";
}
```

When a machine attempts to PXE boot, the DHCP server provides an IP address and the location of the `snponly.efi` (iPXE) binary file on the TFTP server. iPXE then asks the DHCP server for the next file to load, and this time the server returns `mboot.efi` as the filename. iPXE is resident and the system has HTTP capability. As a result, the system can load additional files from an HTTP server.

Example of Booting Using UEFI HTTP with IPv4

This example shows how to configure an ISC DHCP server to boot ESXi by using native UEFI HTTP over IPv4 from Web server `www.example.com`.

```
#
# ISC DHCP server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;
option client-system-arch code 93 = unsigned integer 16;
class "httpclients" {
   match if substring(option vendor-class-identifier, 0, 10) = "HTTPClient";
   option vendor-class-identifier "HTTPClient";

   if option client-system-arch = 00:10 {
      # x86_64 UEFI HTTP client
      filename = http://www.example.com/esxi/mboot.efi;
   }
}
```

Example of Booting Using UEFI HTTP with IPv6

This example shows how to configure an ISC DHCPv6 server to boot ESXi by using native UEFI HTTP over IPv6 from Web server `www.example.com`.

```
#
# ISC DHCPv6 server configuration file snippet.  This is not a complete
# configuration file; see the ISC server documentation for details on
# how to configure the DHCP server.
#
allow booting;
allow bootp;

option dhcp6.bootfile-url code 59 = string;
option dhcp6.user-class code 15 = { integer 16, string };
option dhcp6.vendor-class code 16 = { integer 32, integer 16, string };

if option dhcp6.client-arch-type = 00:10 {
      # x86_64 HTTP clients
      option dhcp6.vendor-class 0 10 "HTTPClient";
      option dhcp6.bootfile-url "http://www.example.com/esxi/mboot.efi";
}
```

Upgrading Hosts by Using ESXCLI Commands

By using ESXCLI, you can upgrade an ESXi 6.5 host or ESXi6.7 host to version 7.0 and update or patch ESXi 6.5, ESXi6.7, and ESXi7.0 hosts.

vSphere 7.0 introduces components, base images, and add-ons as new software deliverables that you can use to update or patch ESXi 7.0 hosts. For information about managing components, base images, and add-ons on ESXi, see ESXCLI Concepts and Examples

To use ESXCLI commands, you must install Standalone ESXCLI. For more information about installing and using ESXCLI, see the following documents.

- Getting Started with ESXCLI
- ESXCLI Reference

Note:

If you press Ctrl+C while an `esxcli` command is running, the command-line interface exits to a new prompt without displaying a message. However, the command continues to run to completion.

For ESXi hosts deployed with vSphere Auto Deploy, the tools VIB must be part of the base booting image used for the initial Auto Deploy installation. The tools VIB cannot be added separately later.

VIBs, Image Profiles, and Software Depots

Upgrading ESXi with esxcli commands requires an understanding of VIBs, image profiles, and software depots.

The following technical terms are used throughout the vSphere documentation set in discussions of installation and upgrade tasks.

VIB	A VIB is an ESXi software package. VMware and its partners package solutions, drivers, CIM providers, and applications that extend the ESXi platform as VIBs. VIBs are available in software depots. You can use VIBs to create and customize ISO images or to upgrade ESXi hosts by installing VIBs asynchronously onto the hosts.
Image Profile	An image profile defines an ESXi image and consists of VIBs. An image profile always includes a base VIB, and might include more VIBs. You examine and define an image profile by using vSphere ESXi Image Builder.
Software Depot	A software depot is a collection of VIBs and image profiles. The software depot is a hierarchy of files and folders and can be available through an HTTP URL (online depot) or a ZIP file (offline depot). VMware and VMware partners make depots available. Companies with large VMware installations might create internal depots to provision ESXi hosts with vSphere Auto Deploy, or to export an ISO for ESXi installation.

Understanding Acceptance Levels for VIBs and Hosts

Each VIB is released with an acceptance level that cannot be changed. The host acceptance level determines which VIBs can be installed to a host.

The acceptance level applies to individual VIBs installed by using the `esxcli software vib install` and `esxcli software vib update` commands, to VIBs installed using vSphere Lifecycle Manager, and to VIBs in image profiles.

The acceptance level of all VIBs on a host must be at least as high as the host acceptance level. For example, if the host acceptance level is VMwareAccepted, you can install VIBs with acceptance levels of VMwareCertified and VMwareAccepted, but you cannot install VIBs with acceptance levels of PartnerSupported or CommunitySupported. To install a VIB with a restrictive acceptance level that is less than the acceptance level of the host, you can change the setting of the host by using the vSphere Client or by running `esxcli software acceptance` commands.

Setting host acceptance levels is a best practice that allows you to specify which VIBs can be installed on a host and used with an image profile, and the level of support you can expect for a VIB. For example, you might set a more restrictive acceptance level for hosts in a production environment than for hosts in a testing environment.

VMware supports the following acceptance levels.

VMwareCertified	The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only I/O Vendor Program (IOVP) program drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.
VMwareAccepted	VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plug-ins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
PartnerSupported	VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
CommunitySupported	The CommunitySupported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs. VIBs at this level have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

Table 35: VIB Acceptance Levels Required to Install on Hosts

Host Acceptance Level	VMwareCertified VIB	VMwareAccepted VIB	PartnerSupported VIB	CommunitySupported VIB
VMwareCertified	x			
VMwareAccepted	x	x		
PartnerSupported	x	x	x	
CommunitySupported	x	x	x	x

Match a Host Acceptance Level with an Update Acceptance Level

You can change the host acceptance level to match the acceptance level for a VIB or image profile that you want to install. The acceptance level of all VIBs on a host must be at least as high as the host acceptance level.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Use this procedure to determine the acceptance levels of the host and the VIB or image profile to install, and to change the acceptance level of the host, if necessary for the update.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Retrieve the acceptance level for the VIB or image profile.

Option	Description
List information for all VIBs	`esxcli --server=<server_name> software sources vib list --depot=<depot_URL>`

Option	Description
List information for a specified VIB	`esxcli --server=<server_name> software sources vib list --viburl=<vib_URL>`
List information for all image profiles	`esxcli --server=<server_name> software sources profile list --depot=<depot_URL>`
List information for a specified image profile	`esxcli --server=<server_name> software sources profile get --depot=<depot_URL> --profile=<profile_name>`

2. Retrieve the host acceptance level.

   ```
   esxcli --server=<server_name> software acceptance get
   ```

3. Optional: If the acceptance level of the VIB is more restrictive than the acceptance level of the host, change the acceptance level of the host.

   ```
   esxcli --server=<server_name> software acceptance set --level=<acceptance_level>
   ```

   The *acceptance_level* can be `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. The values for *acceptance_level* are case-sensitive.

   Note: You can use the --force option for the `esxcli software vib` or `esxcli software profile` command to add a VIB or image profile with a lower acceptance level than the host. A warning will appear. Because your setup is no longer consistent, the warning is repeated when you install VIBs, remove VIBs, and perform certain other operations on the host.

See if ESXi Host Update Requires Maintenance Mode or Reboot

VIBs that you can install with a live install do not require the host to be rebooted, but might require the host to be placed in maintenance mode.

Other VIBs and profiles might require the host to be rebooted after the installation or update.
Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

When you specify a target server by using `--server=<server_name>`, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Check whether the VIB or image profile that you want to install requires the host to be placed in maintenance mode or to be rebooted after the installation or update.

   Run one of the following commands.

Option	Description
Check the VIB	`esxcli --server=<server_name> software sources vib get -v <absolute_path_to_vib>`
Check the VIBs in a depot	`esxcli --server=<server_name> software sources vib get --depot=<depot_name>`
Check the image profile in a depot	`esxcli --server=<server_name> software sources profile get --depot=<depot_name>`

2. Review the return values.

   The return values, which are read from the VIB metadata, indicate whether the host must be in maintenance mode before installing the VIB or image profile, and whether installing the VIB or profile requires the host to be rebooted.

   Note: vSphere Lifecycle Manager relies on an internal ESXi software scan API to determine whether maintenance mode is required or not. When you install a VIB on a live system, if the value for `Live-Install-Allowed` is set to

false, the installation result instructs vSphere Lifecycle Manager to reboot the host. When you remove a VIB from a live system, if the value for `Live-Remove-Allowed` is set to false, the removal result instructs vSphere Lifecycle Manager to reboot the host. In either case, when the remediation starts, vSphere Lifecycle Manager automatically puts the host into maintenance mode.

If necessary, place the host in maintenance mode. See Place a Host in Maintenance Mode. If a reboot is required, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster before the installation or update. Also, place the host in maintenance mode to minimize boot disk activity during the upgrade.

Place a Host in Maintenance Mode

Some installation and update operations that use live install require the host to be in maintenance mode.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Maintenance mode is required when an update operation requires a reboot. However, you only put the host in maintenance mode manually when you use esxcli commands for update and upgrade operations.

To determine whether an upgrade operation requires the host to be in maintenance mode, see See if ESXi Host Update Requires Maintenance Mode or Reboot

Note: If the host is a member of a vSAN cluster, and any virtual machine object on the host uses the "Number of failures to tolerate=0" setting in its storage policy, the host might experience unusual delays when entering maintenance mode. The delay occurs because vSAN has to evacuate this object from the host for the maintenance operation to complete successfully.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Check whether the host is in maintenance mode.

   ```
   esxcli --server=<server_name> system maintenanceMode get
   ```

2. Power off each virtual machine running on the ESXi host.

   Note: You can list all running virtual machines and retrieve the World ID of each one by running the following command.

   ```
   esxcli --server=<server_name> vm process list
   ```

Option	Command
To shut down the guest operating system and then power off the virtual machine	`esxcli --server=<server_name> vm process kill --type soft --world-id <vm_ID>`
To power off the virtual machine immediately	`esxcli --server=<server_name> vm process kill --type hard --world-id <vm_ID>`
To force the power off operation	`esxcli --server=<server_name> vm process kill --type force --world-id <vm_ID>`

   Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

3. Place the host in maintenance mode.

   ```
   esxcli --server=<server_name> system maintenanceMode set --enable true
   ```

4. Verify that the host is in maintenance mode.

   ```
   esxcli --server=<server_name> system maintenanceMode get
   ```

Update a Host with Individual VIBs

You can update a host with VIBs stored in a software depot that is accessible through a URL or in an offline ZIP depot.

- Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.
  See See if ESXi Host Update Requires Maintenance Mode or Reboot. See Place a Host in Maintenance Mode.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

Important: If you are updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update method specified for VMware-supplied depots in the topic Upgrade or Update a Host with Image Profiles.

Note: The `esxcli software vib update` and `esxcli software vib install` commands are not supported for upgrade operations. See Upgrade or Update a Host with Image Profiles.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Determine which VIBs are installed on the host.

   ```
   esxcli --server=<server_name> software vib list
   ```

2. Find out which VIBs are available in the depot.

Option	Description
From a depot accessible by URL	`esxcli --server=<server_name> software sources vib list --depot=http://<web_server>/<depot_name>`
From a local depot ZIP file	`esxcli --server=<server_name> software sources vib list --depot=<absolute_path_to_depot_zip_file>`

   You can specify a proxy server by using the --proxy option.

3. Update the existing VIBs to include the VIBs in the depot or install new VIBs.

Option	Description
Update VIBs from a depot accessible by URL	`esxcli --server=<server_name> software vib update --depot=http://<web_server>/<depot_name>`
Update VIBs from a local depot ZIP file	`esxcli --server=<server_name> software vib update --depot=<absolute_path_to_depot_ZIP_file>`
Install all VIBs from a ZIP file on a specified offline depot (includes both VMware VIBs and partner-supplied VIBs)	`esxcli --server=<server_name> software vib install --depot <path_to_VMware_vib_ZIP_file> \<VMware_vib_ZIP_file> --depot <path_to_partner_vib_ZIP_file>\<partner_vib_ZIP_file>`

   Options for the `update` and `install` commands allow you to perform a dry run, to specify a specific VIB, to bypass the acceptance level verification, and so on. Do not bypass verification on production systems. See the *ESXCLI Reference*.

4. Verify that the VIBs are installed on your ESXi host.

   ```
   esxcli --server=<server_name> software vib list
   ```

Upgrade or Update a Host with Image Profiles

You can upgrade or update a host with image profiles stored in a software depot that is accessible through a URL or in an offline ZIP depot.

- Install Standalone ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.
  See See if ESXi Host Update Requires Maintenance Mode or Reboot. See Place a Host in Maintenance Mode.

  Important: When you use ESXCLI to update or upgrade the host, put the host manually in maintenance mode to ensure that the boot disk is not actively in use before the upgrade begins.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

You can use the `esxcli software profile update` or `esxcli software profile install` command to upgrade or update an ESXi host.

When you upgrade or update a host, the `esxcli software profile update` or `esxcli software profile install` command applies a later version (major or minor) of a full image profile onto the host. After this operation and a reboot, the host can join a vCenter Server environment of the same or later version.

The `esxcli software profile update` command brings the entire content of the ESXi host image to the same level as the corresponding upgrade method using an ISO installer. However, the ISO installer performs a pre-upgrade check for potential problems, such as insufficient memory or unsupported devices. The `esxcli` upgrade method only performs such checks when upgrading from ESXi 6.7 Update 1 or later to a newer version.

For more about the ESXi upgrade process and methods, see Overview of the ESXi Host Upgrade Process.

Important: If you are upgrading or updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware website or downloaded locally, VMware supports only the update command `esxcli software profile update --depot=<depot_location> --profile=<profile_name>`.

When you specify a target server by using `--server=<server_name>`, the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

Note:

Options to the `update` and `install` commands allow you to perform a dry run, to bypass acceptance level verification, to ignore hardware compatibility check warnings, and so on. The option to bypass hardware compatibility check warnings is only available for ESXi 6.7 Update 1 or later. Do not bypass verification on production systems.

For options help, type `esxcli software profile install --help` or `esxcli software profile update --help`. For the complete listing of available command-line options, see the ESXCLI Reference.

1. Determine which VIBs are installed on the host.

   ```
   esxcli --server=<server_name> software vib list
   ```

2. Determine which image profiles are available in the depot.

   ```
   esxcli --server=<server_name> software sources profile list --depot=http://<web_server>/<depot_name>
   ```

   You can specify a proxy server by using the --proxy option.

3. Update the existing image profile to include the VIBs or install new VIBs.

   Important: The `software profile update` command updates existing VIBs with the corresponding VIBs from the specified profile, but does not affect other VIBs installed on the target server. The `software profile install`

command installs the VIBs present in the depot image profile, and removes any other VIBS installed on the target server.

Option	Description
Update the image profile from a VMware-supplied ZIP bundle, in a depot, accessible online from the VMware Web site or downloaded to a local depot	`esxcli software profile update --depot=<depot_location> --profile=<profile_name>` **Important:** This is the only update method that VMware supports for zip bundles supplied by VMware. VMware-supplied ZIP bundle names take the form: `VMware-ESXi-<version_number>-<build_number>-depot.zip`. The profile name for VMware-supplied zip bundles takes one of the following forms. • `ESXi-<version_number>-<build_number>-standard` • `ESXi-<version_number>-<build_number>-notools` (does not include VMware Tools)
Update the image profile from a depot accessible by URL	`esxcli --server=<server_name> software profile update --depot=http://<web_server>/<depot_name> --profile=<profile_name>`
Update the image profile from ZIP file stored locally on the target server	`esxcli --server=<server_name> software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Update the image profile from a ZIP file on the target server, copied into a datastore	`esxcli --server=<server_name> software profile update --depot=<datastore_name>/<profile_ZIP_file> --profile=<profile_name>`
Update the image profile from a ZIP file copied locally and applied on the target server	`esxcli --server=<server_name> software profile update --depot=/<root_dir>/<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Install all new VIBs in a specified profile accessible by URL	`esxcli --server=<server_name> software profile install --depot=http://<web_server>/<depot_name> --profile=<profile_name>`
Install all new VIBs in a specified profile from a ZIP file stored locally on the target.	`esxcli --server=<server_name> software profile install --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
Install all new VIBs from a ZIP file on the target server, copied into a datastore	`esxcli --server=<server_name> software profile install --depot=<datastore_name>/<profile_ZIP_file> --profile=<profile_name>`
Install all new VIBs from a ZIP file copied locally and applied on the target server	`esxcli --server=<server_name> software profile install --depot=/<root_dir>/<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`

4. Verify that the VIBs are installed on your ESXi host.

   ```
   esxcli --server=<server_name> software vib list
   ```

Update ESXi Hosts by Using Zip Files

You can update hosts with VIBs or image profiles by downloading a ZIP file of a depot.

- Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
- Download the ZIP file of a depot bundle from a third-party VMware partner.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.
  See See if ESXi Host Update Requires Maintenance Mode or Reboot. See Place a Host in Maintenance Mode.
- If the update requires a reboot, and if the host belongs to a VMware HA cluster, remove the host from the cluster or disable HA on the cluster.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

Important: If you are updating ESXi from a zip bundle in a VMware-supplied depot, either online from the VMware Web site or downloaded locally, VMware supports only the update method specified for VMware-supplied depots in the topic Upgrade or Update a Host with Image Profiles.

The `esxcli software vib update` and `esxcli software vib install` commands are not supported for upgrade operations. See Upgrade or Update a Host with Image Profiles.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

Install the ZIP file.

```
esxcli --server=<server_name> software vib update --depot=/<path_to_vib_ZIP>/<ZIP_file_name>.zip
```

Remove VIBs from a Host

You can uninstall third-party VIBs or VMware VIBs from your ESXi host.

- If the removal requires a reboot, and if the host belongs to a vSphere HA cluster, deactivate HA for the host.
- Determine whether the update requires the host to be in maintenance mode or to be rebooted. If necessary, place the host in maintenance mode.
  See See if ESXi Host Update Requires Maintenance Mode or Reboot. See Place a Host in Maintenance Mode.

  Important: To ensure that the boot disk is not actively in use when you use ESXCLI to update or upgrade the host, put the host manually in maintenance mode.
- Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

VMware partners prepare third-party VIBs to provide management agents or asynchronously released drivers.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. Power off each virtual machine running on the ESXi host.

   Note: You can list all running virtual machines and retrieve the World ID of each one by running the following command.

   ```
   esxcli --server=<server_name> vm process list
   ```

Option	Command
To shut down the guest operating system and then power off the virtual machine	`esxcli --server=<server_name> vm process kill --type soft --world-id <vm_ID>`
To power off the virtual machine immediately	`esxcli --server=<server_name> vm process kill --type hard --world-id <vm_ID>`

Option	Command
To force the power off operation	`esxcli --server=<server_name> vm process kill --type force --world-id <vm_ID>`

Alternatively, to avoid powering off virtual machines, you can migrate them to another host. See the topic *Migrating Virtual Machines* in the *vCenter Server and Host Management* documentation.

2. Place the host in maintenance mode.

   ```
   esxcli --server=<server_name> system maintenanceMode set --enable true
   ```

3. If necessary, shut down or migrate virtual machines.
4. Determine which VIBs are installed on the host.

   ```
   esxcli --server=<server_name> software vib list
   ```

5. Remove the VIB.

   ```
   esxcli --server=<server_name> software vib remove --vibname=<name>
   ```

   Specify one or more VIBs to remove in one of the following forms.

   - `<name>`
   - `<name>:<version>`
   - `<vendor>:<name>`
   - `<vendor>:<name>:<version>`

   For example, the command to remove a VIB specified by vendor, name and version can take the following form.

   ```
   esxcli --server myEsxiHost software vib remove --vibname=PatchVendor:patch42:version3
   ```

   Note: The `remove` command supports several more options. See the *ESXCLI Reference*.

Add Third-Party Extensions to Hosts with an ESXCLI Command

You can use the `esxcli software vib` command to add a third-party extension released as a VIB package to the system.

When you use this command, the VIB system updates the firewall rule set and refreshes the host daemon after you reboot the system.

Otherwise, you can use a firewall configuration file to specify port rules for host services to enable for the extension. The *vSphere Security* documentation discusses how to add, apply, and refresh a firewall rule set and lists the `esxcli network firewall` commands.

Perform a Dry Run of an ESXCLI Installation or Upgrade

You can use the --dry-run option to preview the results of an installation or upgrade operation. A dry run of the installation or update procedure does not make any changes, but reports the VIB-level operations that will be performed if you run the command without the --dry-run option.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Enter the installation or upgrade command, adding the --dry-run option.
   - `esxcli --server=<server_name> software vib install --dry-run`
   - `esxcli --server=<server_name> software vib update --dry-run`
   - `esxcli --server=<server_name> software profile install --dry-run`
   - `esxcli --server=<server_name> software profile update --dry-run`
2. Review the output that is returned.

   The output shows which VIBs will be installed or removed and whether the installation or update requires a reboot.

List the Available VIBs and Profiles After Host Reboot

You can use the --rebooting-image option to list the VIBs and profiles that are installed on the host and will be active after the next host reboot.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Enter one of the following commands.

Option	Description
For VIBs	`esxcli --server=<server_name> software vib list --rebooting-image`
For Profiles	`esxcli --server=<server_name> software profile get --rebooting-image`

2. Review the output that is returned.

   The output displays information for the ESXi image that will become active after the next reboot. If the pending-reboot image has not been created, the output returns nothing.

Display the Image Profile and Acceptance Level of the Host

You can use the `software profile get` command to display the currently installed image profile and acceptance level for the specified host.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

This command also shows details of the installed image profile history, including profile modifications.

When you specify a target server by using `--server=<server_name>` , the server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with ESXCLI*, or run `esxcli --help` at the ESXCLI command prompt.

1. Enter the following command.

   `esxcli --server=<server_name> software profile get`

2. Review the output.

After You Upgrade ESXi Hosts

To complete a host upgrade, you ensure that the host is reconnected to its managing vCenter Server system and reconfigured if necessary. You also check that the host is licensed correctly.

After you upgrade an ESXi host, take the following actions:

- View the upgrade logs. You can use the vSphere Client to export the log files.
- If a vCenter Server system manages the host, you must reconnect the host to vCenter Server by right-clicking the host in the vCenter Server inventory and selecting **Connect**.
- When the upgrade is complete, the ESXi host is in evaluation mode. The evaluation period is 60 days. You must assign a vSphere 7.0 license before the evaluation period expires. You can upgrade existing licenses or acquire new ones from My VMware. Use the vSphere Client to configure the licensing for the hosts in your environment. See the *vCenter Server and Host Management* documentation for details about managing licenses in vSphere.
- The host sdX devices might be renumbered after the upgrade. If necessary, update any scripts that reference sdX devices.
- Upgrade virtual machines on the host. See Upgrading Virtual Machines and VMware Tools.
- Set up the vSphere Authentication Proxy service. Earlier versions of the vSphere Authentication Proxy are not compatible with vSphere 7.0. See the *vSphere Security* documentation for details about configuring the vSphere Authentication Proxy service.

About ESXi Evaluation and Licensed Modes

You can use evaluation mode to explore a set of features equal to the vSphere Enterprise Plus license.

You can use evaluation mode to explore the entire set of features for ESXi hosts. The evaluation mode provides the set of features equal to a vSphere Enterprise Plus license. Before the evaluation mode expires, you must assign to your hosts a license that supports all the features in use. For example, in evaluation mode, you can use vSphere vMotion technology, the vSphere HA feature, the vSphere DRS feature, and other features. If you want to continue using these features, you must assign a license that supports them.

The installable version of ESXi hosts is always installed in evaluation mode. ESXi Embedded is preinstalled on an internal storage device by your hardware vendor. It might be in evaluation mode or prelicensed.

The evaluation period is 60 days and begins when you turn on the ESXi host. At any time during the 60-day evaluation period, you can convert from evaluation mode to licensed mode. The time available in the evaluation period is decreased by the time already used.

For example, suppose that you use an ESXi host in evaluation mode for 20 days and then assign a vSphere Standard Edition license key to the host. If you set the host back in evaluation mode, you can explore the entire set of features for the host for the remaining evaluation period of 40 days.

For ESXi hosts, license or evaluation period expiry leads to disconnection from vCenter Server. All powered on virtual machines continue to work, but you cannot power on virtual machines after they are powered off. You cannot change the current configuration of the features that are in use. You cannot use the features that remained unused before the license expiration.

For information about managing licensing for ESXi hosts, see the *vCenter Server and Host Management* documentation.

Licensing ESXi Hosts After Upgrade

After you upgrade to ESXi7.0, you must apply a vSphere 7 license.

If you upgrade an ESXi host to a version that starts with the same number, you do not need to replace the existing license with a new one. For example, if you upgrade a host from ESXi 6.5 to 6.7, you can use the same license for the host.

If you upgrade an ESXi host to a version that starts with a different number, you must apply a new license. For example, if you upgrade an ESXi host from 6.x to 7.0, you need to license the host with a vSphere 7 license.

When you upgrade ESXi 6.5 or ESXi6.7 hosts to ESXi7.0 hosts, the hosts are in a 60-day evaluation mode period until you apply the correct vSphere 7 licenses. See About ESXi Evaluation and Licensed Modes.

You can acquire vSphere 7 licenses from My VMware. After you have vSphere 7 licenses, you must assign them to all upgraded ESXi7.0 hosts by using the license management functionality in the vSphere Client. See the *vCenter Server and Host Management* documentation for details. If you use the scripted method to upgrade to ESXi7.0, you can provide the license key in the kickstart (ks) file.

Run the Secure Boot Validation Script on an Upgraded ESXi Host

After you upgrade an ESXi host from an older version of ESXi that did not support UEFI secure boot, you might be able to enable secure boot. Whether you can enable secure boot depends on how you performed the upgrade and whether the upgrade replaced all the existing VIBs or left some VIBs unchanged. You can run a validation script after you perform the upgrade to determine whether the upgraded installation supports secure boot.

- Verify that the hardware supports UEFI secure boot.
- Verify that all VIBs are signed with an acceptance level of at least PartnerSupported. If you include VIBs at the CommunitySupported level, you cannot use secure boot.

For secure boot to succeed, the signature of every installed VIB must be available on the system. Older versions of ESXi do not save the signatures when installing VIBs.

- If you upgrade using ESXCLI commands, the old version of ESXi performs the installation of the new VIBs, so their signatures are not saved and secure boot is not possible.
- If you upgrade using the ISO, new VIBs do have their signatures saved. This is true also for vSphere Lifecycle Manager upgrades that use the ISO.
- If old VIBs remain on the system, the signatures of those VIBs are not available and secure boot is not possible.
  - If the system uses a third-party driver, and the VMware upgrade does not include a new version of the driver VIB, then the old VIB remains on the system after upgrade.
  - In rare cases, VMware might drop ongoing development of a specific VIB without providing a new VIB that replaces or obsoletes it, so the old VIB remains on the system after upgrade.

Note: UEFI secure boot also requires an up-to-date bootloader. This script does not check for an up-to-date bootloader.

1. Upgrade the ESXi and run the following command.

   ```
   /usr/lib/vmware/secureboot/bin/secureBoot.py -c
   ```

2. Check the output.

   The output either includes `Secure boot can be enabled` or `Secure boot CANNOT be enabled.`

Configure Syslog on ESXi Hosts

You can use the vSphere Client, the VMware Host Client, or the `esxcli system syslog` command to configure the syslog service.

The syslog service receives, categorizes, and stores log messages for analyses that help you take preventive action in your environment.

Set ESXi Syslog by using the vSphere Client

You can use the vSphere Client command to configure the syslog service globally and edit various advanced settings.

1. Browse to the ESXi host in the vSphere Client inventory.
2. Click **Configure**.
3. Under **System**, click **Advanced System Settings**.
4. Click **Edit**.
5. Filter for `syslog`.
6. To set up logging globally and configure various advanced settings, see ESXi Syslog Options.
7. Optional: To overwrite the default log size and log rotation for any of the logs:
   a) Click the name of the log that you want to customize.
   b) Enter the number of rotations and the log size you want.
8. Click **OK**.

Changes to the syslog options take effect.

Note: Syslog parameter settings that you define by using the vSphere Client or VMware Host Client are effective immediately. However, most settings you define by using ESXCLI require an additional command to take effect. For more details, see ESXi Syslog Options.

Set ESXi Syslog by using the vSphere Client

You can use the vSphere Client to configure and edit syslog service parameters on ESXi hosts.

1. In the vSphere Client , under **Host**, click **Manage > System > Advanced settings**.
2. In the **Search** panel, type a syslog setting you want to define. See ESXi Syslog Options.
3. Select the setting and click **Edit option**.
4. Set the value as described in the table of parameters in ESXi Syslog Options.
5. Click **Save**.

Set ESXi Syslog by using ESXCLI

You can configure the syslog service on ESXi hosts by using the ESXCLI command: `esxcli system syslog config set <syslog option>`.

For information about using the esxcli system syslog command and other ESXCLI commands, see Getting Started with ESXCLI. For details how to open the ESXi firewall for the port specified in each remote host specification, see ESXi Firewall Configuration.

Note:

Using ESXCLI requires ESXi to open SSH logins, which is a security risk, and is not recommended. If you chose to use ESXCLI, make sure you use the `esxcli system syslog reload` command after setting each parameter to make sure that it takes effect.

Use the ESXCLI command `esxcli system syslog config set <syslog option>` to set a syslog option that you decide to enable. For example, to set the `Syslog.global.logHost` option, use the command `esxcli system syslog config set --loghost=<str>`

After setting `Syslog.global.logHost`, ESXi hosts open and maintain connections to the syslog collectors, and the transmission of messages begins immediately. When ESXi generates a syslog message, it writes it to the appropriate log file on the ESXi host and also forwards it to all configured syslog collectors.

ESXi Syslog Options

You can define the behavior of ESXi syslog files and transmissions by using a set of syslog options.

Apart from the base settings, such as `Syslog.global.logHost`, starting from ESXi 7.0 Update 1, a list of advanced options is available for customizations, and NIAP compliance.

Note: Always configure persistent storage before you set any of the audit record parameters or the `Syslog.global.logDir` parameter.

Note: All audit record settings, beginning with `Syslog.global.auditRecord`, take effect immediately. However, for other settings that you define by using ESXCLI, make sure to run the `esxcli system syslog reload` command to enable the changes.

Table 36: Legacy Syslog Options

Option	ESXCLI command	Description
`Syslog.global.logHost`	`esxcli system syslog config set --loghost=<str>`	Defines a comma-delimited list of remote hosts and specifications for message transmissions. If the `loghost=<str>` field is blank, no logs are forwarded. While no hard limit to the number of remote hosts to receive syslog messages exists, good practice is to keep the number of remote hosts to five or less. The format of a remote host specification is: `protocol://hostname|ipv4|'['ipv6']'[:port][?formatter=value[&framing=value]]`. The protocol must be one of `tcp`,`udp`, or `ssl`. The value of a port can be any decimal number between 1 and 65535. If a port is not provided, UDP and TCP use 514; SSL uses 1514. For example: `ssl://hostName1:1514`. The formatter must be RFC_3164 or RFC_5424; RFC_3164 is the default. The framing must be `non_transparent` or `octet_counting`; the default is `non_transparent`. For more information, see Fine-tune Syslog on ESXi Hosts.
`Syslog.global.defaultRotate`	`esxcli system syslog config set --default-rotate=<long>`	Maximum number of old log files to keep. You can set this number globally and for individual subloggers (see `Syslog.global.defaultSize`).

Option	ESXCLI command	Description
Syslog.global.defaultSize	esxcli system syslog config set --default-size=<long>	Default size of log files, in KiB. After a file reaches the default size, the syslog service creates a new file. You can set this number globally and for individual subloggers.
Syslog.global.logDir	esxcli system syslog config set --logdir=<str>	Directory where logs reside. The directory can be on mounted NFS or VMFS volumes. Only the /scratch directory on the local file system is persistent across reboots. Specify the directory as [*datastorename*] *path_to_file*, where the path is relative to the root of the volume backing the datastore. For example, the path [storage1] /systemlogs maps to the path /vmfs/volumes/storage1/systemlogs.
Syslog.global.logDirUnique	esxcli system syslog config set --logdir-unique=<bool>	Specifies the ESXi host name to be concatenated to the value of Syslog.global.logDir. It is critical that you enable this setting when multiple ESXi hosts log to a shared file system. Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.certificate.checkSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	Enforces checking of SSL certificates when transmitting messages to remote hosts.

Table 37: Syslog Options Available Starting from ESXi 7.0 Update 1

Option	ESXCLI command	Description
Syslog.global.auditRecord.storageCapacity	esxcli system auditrecords local set --size=<long>	Specifies the capacity of the audit record storage directory located on the ESXi host, in MiB. You cannot decrease the capacity of the audit record storage. You can increase the capacity before or after the audit record storage is enabled (see Syslog.global.auditRecord.storageEnable).
Syslog.global.auditRecord.remoteEnable	esxcli system auditrecords remote enable	Enables sending audit records to remote hosts. Remote hosts are specified by using the Syslog.global.logHost parameter.

Option	ESXCLI command	Description
Syslog.global.auditRecord.storageDirectory	esxcli system auditrecords local set --directory=<dir>	Creates an audit record storage directory and unless specified, sets /scratch/auditLog as the default location. You must not manually create an audit record storage directory and you cannot change the audit record storage directory while audit record storage is enabled (see Syslog.global.auditRecord.storageEnable).
Syslog.global.auditRecord.storageEnable	esxcli system auditrecords local enable	Enables the storage of audit records on an ESXi host. If the audit record storage directory does not exist, it is created with the capacity specified by Syslog.global.auditRecord.storageCapacity.
Syslog.global.certificate.checkCRL	esxcli system syslog config set --crl-check=<bool>	Enables checking the revocation status of all the certificates in an SSL certificate chain. Enables verification of X.509 CRLs, which are not checked by default in compliance with industry conventions. A NIAP-validated configuration requires CRL checks. Due to implementation limitations, if CRL checks are enabled, then all certificates in a certificate chain must provide a CRL link. Do not enable the crl-check option for installations not related to certification, because of the difficulty in properly configuring an environment that uses CRL checks.
Syslog.global.certificate.strictX509Compliance	esxcli system syslog config set --x509-strict=<bool>	Enables strict compliance with X.509. Performs additional validity checks on CA root certificates during verification. These checks are generally not performed, as CA roots are inherently trusted, and might cause incompatibilities with existing, misconfigured CA roots. A NIAP-validated configuration requires even CA roots to pass validations. Do not enable the x509-strict option for installations not related to certification, because of the difficulty in properly configuring an environment that uses CRL checks.
Syslog.global.droppedMsgs.fileRotate	esxcli system syslog config set --drop-log-rotate=<long>	Specifies the number of old dropped message log files to keep.
Syslog.global.droppedMsgs.fileSize	esxcli system syslog config set --drop-log-size=<long>	Specifies the size of each dropped message log file before switching to a new one, in KiB.
Syslog.global.logCheckSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	Enforces checking of SSL certificates when transmitting messages to remote hosts.

Option	ESXCLI command	Description
		Note: Deprecated. Use `Syslog.global.certificate.checkSSLCerts` in ESXi 7.0 Update 1 and later.
`Syslog.global.logFilters`	`esxcli system syslog config logfilter [add | remove | set] ...`	Specifies one or more log filtering specifications. Each log filter must be separated by a double vertical bar "||". The format of a log filter is: `numLogs | ident | logRegexp`. `numLogs`sets the maximum number of log entries for the specified log messages. After reaching this number, the specified log messages are filtered and ignored. `ident` specifies one or more system components to apply the filter to the log messages that these components generate. `logRegexp` specifies a case-sensitive phrase with Python regular expression syntax to filter the log messages by their content.
`Syslog.global.logFiltersEnable`		Enables the use of log filters.
`Syslog.global.logLevel`	`esxcli system syslog config set --log-level=<str>`	Specifies the log filtering level. You must change this parameter only when troubleshooting an issue with the syslog daemon. You can use the values `debug` for the most detailed level, `info` for the default detail level, `warning` for only warnings or errors, or `error`, only for errors.
`Syslog.global.msgQueueDropMark`	`esxcli system syslog config --queue-drop-mark=<long>)`	Specifies the percent of the message queue capacity at which messages are dropped.
`Syslog.global.remoteHost.connectRetryDelay`	`esxcli system syslog config set --default-timeout=<long>`	Specifies the delay before retrying to connect to a remote host after a connection attempt fails, in seconds.
`Syslog.global.remoteHost.maxMsgLen`	`esxcli system syslog config set --remote-host-max-msg-len=<long>`	For the TCP and SSL protocols, this parameter specifies the maximum length of a syslog transmission before truncation occurs, in bytes. The default maximum length for remote host messages is 1 KiB. You can increase the maximum message length to up to 16 KiB. However, raising this value above 1 KiB does not ensure that long transmissions arrive untruncated to a syslog collector. For example, when the syslog infrastructure that issues a message is external to ESXi. This setting does not affect the UDP protocol. RFC 5426 specifies the UDP message lengths that can be safely accepted at 480 bytes for IPV4 and 1180 bytes for IPV6. Because of

Option	ESXCLI command	Description
		these restrictions, and because the networking infrastructure can arbitrary drop UDP packets, the use of UDP for transmitting critical syslog messages is not recommended.
`Syslog.global.vsanBacking`	`esxcli system syslog config set --vsan-backing=<bool>`	Allows log files and the audit record storage directory to be placed on a vSAN cluster. However, enabling this parameter might cause the ESXi host to become unresponsive.

Fine-tune Syslog on ESXi Hosts

By using the right syslog settings, you can achieve proactive monitoring of your environment, reduce downtime and take preventive action on servers.

While setting up syslog, you need to consider several parameters that affect log file retention, syslog transmission, transmission length, error handling, and the set up of SSL certificates for secure syslog message transmission. What follows are recommendations for fine-tuning your syslog parameters. You can see a description of all available parameters at ESXi Syslog Options.

How to Specify Log File Retention

By default, log files cannot expand past a configured size. Once a log file reaches the configured size, logging is routed to a new log file and the oldest log file is deleted.

Note: Best practice is to balance the rotate and size settings. Increasing the rotate setting ensures that syslog files are generated often enough to prevent any potential corruption or destruction from the other log files. Increasing the size setting reduces the time for switching to another log file. Optimal size settings are a multiple of 1024 KiB.

Use the Syslog.global.defaultSize setting to specify the log file maximum size in KiB, and Syslog.global.defaultRotate to set the maximum number of old log files to keep before rotating to a new log file. To change the log file retention parameters associated with a specific program, use the `Syslog.loggers.<progName>.rotate` and `Syslog.loggers.<progName>.size settings`, where `<progName>` is the name of the program whose parameters you want to adjust.

Manage Settings that Affect the Virtual Machine Log File

You can configure some settings that affect the virtual machine log file, `vmware.log`, either in the `vmx` file or in the `/etc/vmware/config` file. You must power off a virtual machine to edit the `vmx` file and edits take effect only on that virtual machine. If you use the `/etc/vmware/config` file, you must add the prefix *"vmx"* to the setting, for example `vmx.log.keepOld = "20"` , and edits affect all virtual machines on the ESXi host.

Table 38: Configurable settings for the vmware.log file

Parameter	Description	Example	Notes
`logging`	Disables all virtual machine logging.	The default value is `logging = "TRUE"` To disable virtual machine logging: `logging = "FALSE"`	Do not use this setting, because disabling virtual machine logging makes it difficult or impossible to get support for virtual machine problems. If you need to use this setting for some reason, you can only place it in the `vmx` file of a virtual machine.
`log.throttleBytesPerSec`	Controls when a log file throttles. Log file throttling occurs when writes to the `vmware.log` exceed the specified rate for a significant amount of time. This occurs when code within the VMX process, which controls a virtual machine, creates excessive log messages. The default value for this setting is 1 KB/sec. In case of log thottling, you see `<<< Log Throttled >>>` in the `vmware.log` file.	`log.throttleBytesPerSec = "1500"` To disable log throttling, use `log.throttleBytesPerSec = "0xFFFFFFFF"`	Log file thottling might obscure information necessary to diagnose problems with the affected virtual machine. If you need to disable log throttling, place the line in the example in the `vmx` file of the affected virtual machine. Remove the line after the debugging session ends.
`log.keepOld`	Controls the number of older `vmware.log` file to retain.	`log.keepOld = "20"`	Do not put the value of this setting below the default value (10). If virtual machines are frequently modified or moved, consider raising this setting to 20 or more.
`log.rotateSize`	Controls the maximum size of a `vmware.log` file in bytes.	`log.rotateSize = "2500000"` To disable limiting the maximum size of a `vmware.log` file, use `log.rotateSize = "0"`	A value of this setting below 100,000 can cause a loss of critical log messages and affect virtual machine performance. In ESXi 7.x and earlier, the default value of this setting places no limit on the size of a `vmware.log` file. In ESXi 8.x and later, the default value of this setting is 2,048,000.

`log.fileName`	Controls the name and location of virtual machine log files.	`log.fileName = "myVMLog"`
		This setting changes the name of the virtual machine log files from vmware.log to `myVMlog`.
		`log.fileName = "/vmfs/volumes/vol1/myVM/myVM.log"`
			Do not place a log file outside the virtual machine directory to make sure that the collection of host support bundles picks up the log file, which can be critical to debug virtual machine problems.

Parameter	Description	Example	Notes
		This setting directs virtual machine log files to a directory on a different VMFS volume (vol1) by using `myVM` for a file name.	
`log.fileLevel`	Controls the minimum level at which messages are written to `vmware.log`. Every log message has a level associated with it. Levels below the specified setting are not added to a virtual machine log file. The virtual machine message log levels (from most to least restricted) are: • error • warning • notice • info (default) • trivia • debug • debug1 • debug2 • debug3 • debug4 • debug5 • debug6 • debug7 • debug8 • debug9 • debug10	`log.fileLevel = "debug1"`	Do not set a more restrictive level than "info" to avoid filtering out messages that are necessary for debugging virtual machine problems. Lower the level below "info" only upon request by licensed support. Restore the setting to "info" after debugging ends.
`log.filter.minLogLevel.<groupName>`	Controls the output of specialized debugging messages.	`log.filter.minLogLevel.<groupName> = "debug5"`	Use this setting only upon request by licensed support, who should provide one or more `<groupName>` parameters. Remove the setting after debugging ends.
`log.sysogID`	Activates the sending of virtual machine log messages to the system logger of an ESXi host, such as the syslog.	`log.syslogID = "vmx"`	Use `"vmx"` as value for this setting to allow the ESXi syslog daemon, `vmsyslogd`, to send these messages to a separate log file.
`log.syslogLevel`	Controls the minimum level at which messages are output to the system logger of an ESXi host, such as the syslog.	`log.syslogLevel = "debug"`	The levels and functioning of this setting are identical to those for the `log.fileLevel` setting.

How to Specify Message Transmission to Remote Hosts

Optionally, you can configure ESXi to send syslog messages to one or more remote hosts, called syslog collectors, such as VMware Aria Operations for Logs (formerly VMware vRealize Log Insight and vCenter Log Insight), to collect syslog messages.

Note: Best practice is that you configure each ESXi host to send syslog messages to at least one syslog collector. This helps ensure that the messages are preserved in case of a catastrophic system event and that you can process syslog messages in various ways, such as real-time categorization and analysis (for example, by type, time span, or machine), or archive messages.

Use the `Syslog.global.logHost` setting to define remote host specifications. Separate multiple remote host specifications with a comma (,). After setting `Syslog.global.logHost`, ESXi hosts open and maintain connections to the syslog collectors, and the transmission of messages begins immediately. When ESXi generates a syslog message, it writes it to the appropriate log file on the ESXi host and also forwards it to all configured syslog collectors.

In addition to syslog messages, audit messages can also be transmitted to syslog collectors for security purposes. Audit records track security-related activity on the ESXi host. For more information about audit records, see Audit Records.

Note: Consult with your company security response team if and how to set audit records. Certified configurations usually require audit records to be activated.

What follows is the syntax for `Syslog.global.logHost` remote host specifications:

```
protocol://target[:port]
```

Parameter	Description	Notes
`protocol`	Specifies the networking protocol. Valid values are `udp`, `tcp`, and `ssl`.	The `ssl` protocol specifies that transmission of syslog messages is encrypted. The `tcp` and `udp` protocols do not encrypt the transmission. **Note:** If capturing syslog messages or audit messages is critical to your system, avoid using the `udp` protocol because the networking infrastructure external to ESXi might drop UDP messages.
`target`	Specifies the remote host. You can use either an IPV4 or IPV6 address, or a host name.	When you use an IPV6 address, you must embed it in square brackets `[xxx]`, where `xxx` is the IPV6 address.
`port`	(Optional) Specifies the remote host port to use. If you use UDP or TCP, the default port is 514. If you use SSL, the default port is 1514. If you choose to use different ports from 514 or 1514, you must adjust the ESXi firewall to open the port.	For details how to open the ESXi firewall for the port specified in each remote host specification, see ESXi Firewall Configuration.

Examples of remote machine specifications:

Syslog.global.logHost string example	Notes
tcp://10.176.130.7:12345	Transmits syslog messages to 10.176.130.7 using TCP/IP and port 12345.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]	Transmits syslog messages to an IPV6 address using port 1514.
tcp://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:5432	Transmit syslog messages to an IPV6 address using port 54321.

Syslog.global.logHost string example	Notes
udp://company.com	Transmits syslog messages to `company.com` using UDP and port 514.
udp://company.com,tcp://10.20.30.40:1050	Transmits syslog messages to two remote hosts. The first remote host uses UDP to communicate with `company.com` using port 514. The second remote host uses TCP to communicate with the IPV4 address `10.20.30.40` using port 1050.
ssl://company.com	Transmits syslog messages to `company.com` using SSL (TLS) and port 514.

Maximum Message Transmission Length

If you use UDP, the maximum syslog message transmission length is 480 bytes for IPV4 and 1180 bytes for IPV6.

For TCP or SSL, the default maximum syslog message transmission length is 1 kibibyte (KiB). You can increase this length by using the `Syslog.global.remoteHost.maxMsgLen` parameter. The maximum value is 16 KiB. Messages longer than 16 KiB are truncated.

Note: If increasing the maximum transmission length is necessary, best practice is to increase the length only as much as specifically necessary.

Increasing the maximum syslog message length can cause problems if the networking and syslog infrastructure external to ESXi is unable to handle messages longer than 1 KiB.

Note: Best practice is that you do not use UDP to transmit syslog messages due to the packet length constraints and the possibility that the external networking infrastructure might drop the messages.

Considerations for Certificates When Configuring SSL Transmissions to Remote Hosts

When configuring ESXi to transmit syslog messages to remote hosts using SSL, you must add an SSL certificate for each remote host to the ESXi host CA store. For more information, see Certificate Management for ESXi Hosts and Manage CA Certificates with ESXCLI.

Note: Consult with your syslog collector documentation on how to configure the collector for secure receipt of syslog messages using SSL and a private key.

Additional SSL Transmission Parameters

An ESXi system complying with security certification requirements might require activating X509 CRL checks. You turn on the advanced settings `Syslog.global.certificate.strictX509Compliance` and `Syslog.global.certificate.checkCRL` by changing the default value of `false` to `true`. Due to implementation limitations, if you activate CRL checks by using the setting `Syslog.global.certificate.checkSSLCerts`, then all certificates in a certificate chain must provide a CRL link. By default, the setting is active. You can deactivate SSL certificate checks by changing the setting to `false`, but this is not a best practice. You might need to turn off SSL certificate checks when troubleshooting communications with a remote host, but do this only for a limited time.

Where to Find Syslog Daemon Error and Status Information

The ESXi syslog daemon uses the log file `/var/run/log/vmsyslogd.log` to store status and error information, including dropped messages. If audit record transmission is active, the syslog daemon also emits audit records related to its operation, such as daemon start, stop, and error conditions, which allows you to verify that the syslog daemon runs properly.

How to Change the Default Syslog Log File Storage Area

The default syslog log file storage area is `/var/run/log`, local to each ESXi host. Use the `Syslog.global.logDir` syslog configuration variable to change the default syslog log file storage area, as long as the location resides on persistent storage. If `Syslog.global.logDir` is configured to a persistent store shared by multiple ESXi hosts to store their syslog log files, change the `Syslog.global.logDirUnique` setting to `true` to prevent mixing logs. The `Syslog.global.logDirUnique` setting makes sure that each ESXi machine gets a unique name added to the `Syslog.global.logDir` path, separating the log files from other hosts.

Syslog Message Queueing for Remote Hosts and Message Drops

Once syslog emissions start, they never stop except for ESXi reboots and failures, or a syslog reconfiguration to stop.

To avoid dropping messages, ESXi uses an in-memory queue that allows the `vmsyslogd` service to handle the following conditions for a short time:

- ESXi generates log messages at a faster rate than the `vmsyslogd` service can process and transmit
- Network connectivity between ESXi and the remote host fails

If either of these conditions continues for a long period, the capacity of the in-memory queue might not be sufficient and `vmsyslog` might stop transmitting messages and audit logs to remote hosts. No data is lost, because dropped messages are written to the `/var/run/log/vmsyslogd-dropped.log` file.

To minimize the chance that message dropping occurs, place the `vmsyslogd` log files on the fastest available storage and configure `vmsyslogd` and its syslog collectors on a network with end-to-end bandwidth greater than 1 GigE.

Note: Consider an end-to-end bandwidth of 2.5 GigE or more, preferably 10 GigE, to optimize performance and prevent message drops.

If you see excessive logs from an application, file a support service request for analysis and correction.

You can see statistics about message drops in the syslog daemon log file.

You can see dropped messages at `/var/run/log/vmsyslogd-dropped.log`. This log file has retention settings specific to it, similar to those for the program-specific retention parameters. The dropped messages log file retention parameters are: `Syslog.global.droppedMsgs.fileRotate` and `Syslog.global.droppedMsgs.fileSize`.

Configure Log Filtering on ESXi Hosts

The log filtering capability lets you modify the logging policy of the syslog service that is running on an ESXi host.

You can create log filters to reduce the number of repetitive entries in the ESXi logs and to denylist specific log events entirely.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Starting with vSphere 7.0 Update 2, you can add log filters and enable log filtering by using ESXCLI. A log filter, once established, remains in place until it is removed, even across ESXi reboots.

Log filters affect all log events that are processed by the ESXi host `vmsyslogd` service, whether they are recorded to a log directory or to a remote syslog server.

You must enable the log filtering capability and reload the syslog daemon to activate the log filters on the ESXi host.

ESXCLI commands to configure log filters follow this pattern: `esxcli system syslog config logfilter {cmd} [cmd options]`.

For example, to get the list of available log filters, run the following command: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter list`.

Use the `set` command to activate or deactivate log filtering: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter set`.

Use the `add` command to add a log filter and the `remove` command to remove a log filter.

Use the `get` command to determine if log filtering is enabled.

A log filter is specified by three components and uses the following syntax: `numLogs | ident | logRegexp` .

Parameter	Description
`numLogs`	Specifies the number of matches of the logRegexp Python regular expression that will be allowed before filtering begins.
`ident`	The `ident` string is how an application identifies itself to the syslog facility. The `logRegexp` filter must be associated with the same application. You can find the `ident` string of an application by inspecting the log files in `/var/run/log`. The third field of each log file begins with the `ident` string and ends with `[`.
`logRegexp`	Python regular expression that identifies the messages which you want to filter out.

For example, to filter out all messages from the hostd daemon that contain the word "mark" after the tenth occurrence, use the following command: `esxcli system syslog config logfilter add --filter="10|Hostd|mark"` .

To remove the log filter, use the command `esxcli system syslog config logfilter remove --filter="10|Hostd|mark"`.

For more information, see ESXi Syslog Options.

Using vSphere Auto Deploy to Reprovision Hosts

You can reprovision ESXi hosts deployed by using vSphere Auto Deploy with a new image profile for a different version of ESXi.

Note: If you upgrade the host to use an ESXi 6.0 or later image, the vSphere Auto Deploy server provisions the ESXi host with certificates that are signed by VMCA. If you are currently using custom certificates, you can set up the host to use the custom certificates after the upgrade. See *vSphere Security*.

If a host was deployed using vSphere Auto Deploy, you can use vSphere Auto Deploy to reprovision the host with a new image profile that contains a different version of ESXi. You can use vSphere ESXi Image Builder to create and manage image profiles. The vSphere Auto Deploy server is automatically upgraded if you upgrade the corresponding vCenter Server system. Starting with version 6.0, the vSphere Auto Deploy server is always on the same management node as the vCenter Server system.

Introduction to vSphere Auto Deploy

When you start a physical host that is set up for vSphere Auto Deploy, vSphere Auto Deploy uses PXE boot infrastructure in conjunction with vSphere host profiles to provision and customize that host. No state is stored on the host itself. Instead, the vSphere Auto Deploy server manages state information for each host.

State Information for ESXi Hosts

vSphere Auto Deploy stores the information for the ESXi hosts to be provisioned in different locations. Information about the location of image profiles and host profiles is initially specified in the rules that map machines to image profiles and host profiles.

Table 39: vSphere Auto Deploy Stores Information for Deployment

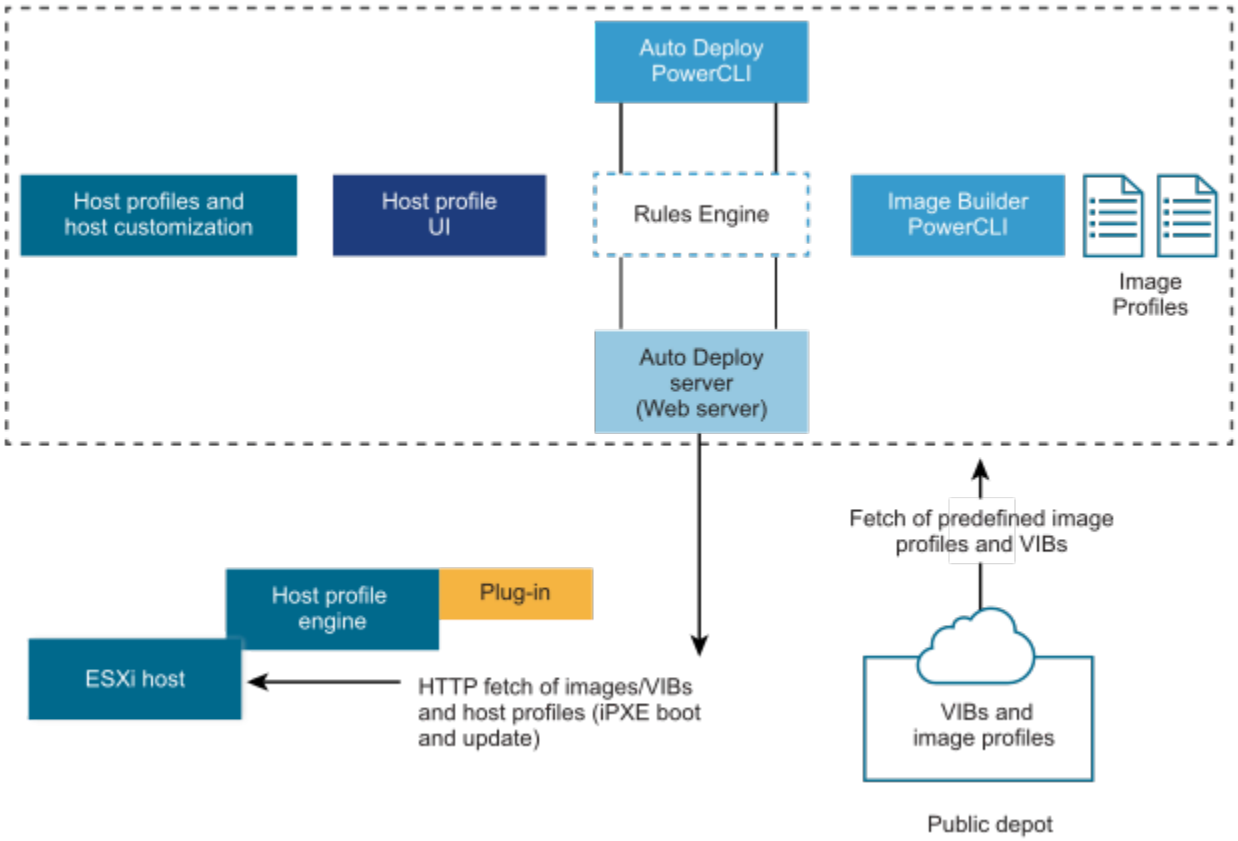
Information Type	Description	Source of Information
Image state	The executable software to run on an ESXi host.	Image profile, created with vSphere ESXi Image Builder.
Configuration state	The configurable settings that determine how the host is configured, for example, virtual switches and their settings, driver settings, boot parameters, and so on.	Host profile, created by using the host profile UI. Often comes from a template host.
Dynamic state	The runtime state that is generated by the running software, for example, generated private keys or runtime databases.	Host memory, lost during reboot.
Virtual machine state	The virtual machines stored on a host and virtual machine autostart information (subsequent boots only).	Virtual machine information sent by vCenter Server to vSphere Auto Deploy must be available to supply virtual machine information to vSphere Auto Deploy.
User input	State that is based on user input, for example, an IP address that the user provides when the system starts up, cannot automatically be included in the host profile.	Host customization information, stored by vCenter Server during first boot. You can create a host profile that requires user input for certain values. When vSphere Auto Deploy applies a host profile that requires user provided information, the host is placed in maintenance mode. Use the host profile UI to check the host profile compliance, and respond to the prompt to customize the host.

vSphere Auto Deploy Architecture

The vSphere Auto Deploy infrastructure consists of several components.

For more information, watch the video "Auto Deploy Architecture":

Figure 16: vSphere Auto Deploy Architecture



vSphere Auto Deploy server
Serves images and host profiles to ESXi hosts.

vSphere Auto Deploy rules engine

Image profiles
Define the set of VIBs to boot ESXi hosts with.

- VMware and VMware partners make image profiles and VIBs available in public depots. Use vSphere ESXi Image Builder to examine the depot and use the vSphere Auto Deploy rules engine to specify which image profile to assign to which host.

Host profiles

Host customization
Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host. For more information about host customizations, see the *vSphere Host Profiles* documentation.

Host customization was called answer file in earlier releases of vSphere Auto Deploy.

Preparing for vSphere Auto Deploy

Before you can start using vSphere Auto Deploy, you must prepare your environment. You start with server setup and hardware preparation. You must configure the vSphere Auto Deploy service startup type in the vCenter Server system that you plan to use for managing the hosts you provision, and install PowerCLI.

Prepare Your System for vSphere Auto Deploy

Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.

- Verify that the hosts that you plan to provision with vSphere Auto Deploy meet the hardware requirements for ESXi. See ESXi Hardware Requirements.
- Verify that the ESXi hosts have network connectivity to vCenter Server and that all port requirements are met. See *vCenter Server Upgrade*.
- Verify that you have a TFTP server and a DHCP server in your environment to send files and assign network addresses to the ESXi hosts that Auto Deploy provisions. See Install the TFTP Server and Prepare the DHCP Server for vSphere Auto Deploy Provisioning.
- Verify that the ESXi hosts have network connectivity to DHCP, TFTP, and vSphere Auto Deploy servers.
- If you want to use VLANs in your vSphere Auto Deploy environment, you must set up the end to end networking properly. When the host is PXE booting, the firmware driver must be set up to tag the frames with proper VLAN IDs. You must do this set up manually by making the correct changes in the UEFI/BIOS interface. You must also correctly configure the ESXi port groups with the correct VLAN IDs. Ask your network administrator how VLAN IDs are used in your environment.
- Verify that you have enough storage for the vSphere Auto Deploy repository. The vSphere Auto Deploy server uses the repository to store data it needs, including the rules and rule sets you create and the VIBs and image profiles that you specify in your rules.

  Best practice is to allocate 2 GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 400 MB. Determine how much space to reserve for the vSphere Auto Deploy repository by considering how many image profiles you expect to use.
- Obtain administrative privileges to the DHCP server that manages the network segment you want to boot from. You can use a DHCP server already in your environment, or install a DHCP server. For your vSphere Auto Deploy setup, replace the `gpxelinux.0` filename with `snponly64.efi.vmw-hardwired` for UEFI or `undionly.kpxe.vmw-hardwired` for BIOS. For more information on DHCP configurations, see Sample DHCP Configurations.
- Secure your network as for any other PXE-based deployment method. vSphere Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or the vSphere Auto Deploy server is not checked during a PXE boot.
- If you want to manage vSphere Auto Deploy with PowerCLI cmdlets, verify that Microsoft .NET Framework 4.5 or 4.5.x and Windows PowerShell 3.0 or 4.0 are installed on a Windows machine. See the *vSphere PowerCLI User's Guide*.
- Set up a remote Syslog server. See the *vCenter Server and Host Management* documentation for Syslog server configuration information. Configure the first host you boot to use the remote Syslog server and apply that host's host profile to all other target hosts. Optionally, install and use VMware vCenter Log Insight, which provides log aggregation and analytics for VMware and non-VMware products, virtual and physical, with near real-time search and analytics of log events.
- If the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, verify that the vSphere Auto Deploy server has an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

If you want to manage vSphere Auto Deploy with PowerCLI cmdlets, see *Set Up vSphere Auto Deploy and Provision Hosts with vSphere PowerCLI*.

1. Navigate to **Home** > **Auto Deploy**.

   By default, only the administrator role has privileges to use the vSphere Auto Deploy service.
2. On the **Auto Deploy** page, select your vCenter Server from the drop-down menu at the top.
3. Click **Enable Auto Deploy and Image Builder** to activate the service.

   If the **Image Builder** service is already active, select the **Configure** tab and click **Enable Auto Deploy Service**.

   The **Software Depot** page appears.

4. Configure the TFTP server.
   a) Click the **Configure** tab.
   b) Click **Download TFTP Boot Zip** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.
   c) Optional: To use a proxy server, click **Add** on the *Auto Deploy Runtime Summary* pane and enter a proxy server URL in the text box.

      Using reverse proxy servers can offload the requests made to the vSphere Auto Deploy server.
5. Set up your DHCP server to point to the TFTP server on which the TFTP ZIP file is located.
   a) Specify the TFTP Server's IP address in DHCP option 66, frequently called next-server.
   b) Specify the boot filename, which is `snponly64.efi.vmw-hardwired` for UEFI or `undionly.kpxe.vmw-hardwired` for BIOS in the DHCP option 67, frequently called `boot-filename`.
6. Set each host you want to provision with vSphere Auto Deploy to network boot or PXE boot, following the manufacturer's instructions.
7. Optional: If you set up your environment to use Thumbprint mode, you can use your own Certificate Authority (CA) by replacing the OpenSSL certificate `rbd-ca.crt` and the OpenSSL private key `rbd-ca.key` with your own certificate and key file.

   The files are in `/etc/vmware-rbd/ssl/`.

   By default, vCenter Server uses VMware Certificate Authority (VMCA).

When you start an ESXi host that is set up for vSphere Auto Deploy, the host contacts the DHCP server and is directed to the vSphere Auto Deploy server, which provisions the host with the image profile specified in the active rule set.

- You can change the default configuration properties of the **Auto Deploy Service**. For more information, see "Configuring vCenter Server" in the *vCenter Server and Host Management* documentation.
- You can change the default configuration properties of the **Image Builder Service**. For more information, see "Configuring vCenter Server" in the *vCenter Server and Host Management* documentation.
- Configure the first host that you provision as a reference host. Use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for the reference host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- If you have to configure host-specific information, set up the host profile of the reference host to prompt for user input. For more information about host customizations, see the *vSphere Host Profiles* documentation.

Related Links

Using vSphere Auto Deploy Cmdlets on page 1232

vSphere Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. Users of vSphere Auto Deploy cmdlets can take advantage of all PowerCLI features.

Set Up Bulk Licensing on page 1233

You can use the vSphere Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with vSphere Auto Deploy.

Using vSphere Auto Deploy Cmdlets

vSphere Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. Users of vSphere Auto Deploy cmdlets can take advantage of all PowerCLI features.

Experienced PowerShell users can use vSphere Auto Deploy cmdlets just like other PowerShell cmdlets. If you are new to PowerShell and PowerCLI, the following tips might be helpful.

You can type cmdlets, parameters, and parameter values in the PowerCLI shell.

- Get help for any cmdlet by running `Get-Help`*`cmdlet_name`* .
- Remember that PowerShell is not case sensitive.
- Use tab completion for cmdlet names and parameter names.
- Format any variable and cmdlet output by using `Format-List` or `Format-Table`, or their short forms `fl` or `ft`. For more information, run the `Get-Help Format-List` cmdlet.

Passing Parameters by Name

You can pass in parameters by name in most cases and surround parameter values that contain spaces or special characters with double quotes.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

Most examples in the *vCenter Server Installation and Setup* documentation pass in parameters by name.

Passing Parameters as Objects

You can pass parameters as objects if you want to perform scripting and automation. Passing in parameters as objects is useful with cmdlets that return multiple objects and with cmdlets that return a single object. Consider the following example.

1. Bind the object that encapsulates rule set compliance information for a host to a variable.
   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```
2. View the `itemlist` property of the object to see the difference between what is in the rule set and what the host is currently using.
   ```
   $tr.itemlist
   ```
3. Remediate the host to use the revised rule set by using the `Repair-DeployRuleSetCompliance` cmdlet with the variable.
   ```
   Repair-DeployRuleSetCompliance $tr
   ```

The example remediates the host the next time you boot the host.

Related Links

Prepare Your System for vSphere Auto Deploy on page 1231
Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.

Set Up Bulk Licensing on page 1233
You can use the vSphere Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with vSphere Auto Deploy.

Set Up Bulk Licensing

You can use the vSphere Client or ESXi Shell to specify individual license keys, or you can set up bulk licensing by using PowerCLI cmdlets. Bulk licensing works for all ESXi hosts, but is especially useful for hosts provisioned with vSphere Auto Deploy.

#unique_200.

Assigning license keys through the vSphere Client and assigning licensing by using PowerCLI cmdlets function differently.

Assign license keys with the vSphere Client	You can assign license keys to a host when you add the host to the vCenter Server system or when the host is managed by a vCenter Server system.

Assign license keys with LicenseDataManager PowerCLI	You can specify a set of license keys to be added to a set of hosts. The license keys are added to the vCenter Server database. Each time a host is added to the vCenter Server system or reconnects to it, the host is assigned a license key. A license key that is assigned through PowerCLI is treated as a default license key. When an unlicensed host is added or reconnected, it is assigned the default license key. If a host is already licensed, it keeps its license key.

The following example assigns licenses to all hosts in a data center. You can also associate licenses with hosts and clusters.

The following example is for advanced PowerCLI users who know how to use PowerShell variables.

1. In a PowerCLI session, connect to the vCenter Server system you want to use and bind the associated license manager to a variable.

   ```
   Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
   $licenseDataManager = Get-LicenseDataManager
   ```

2. Run a cmdlet that retrieves the data center in which the hosts for which you want to use the bulk licensing feature are located.

   ```
   $hostContainer = Get-Datacenter -Name Datacenter-X
   ```

   You can also run a cmdlet that retrieves a cluster to use bulk licensing for all hosts in a cluster, or retrieves a folder to use bulk licensing for all hosts in a folder.

3. Create a `LicenseData` object and a `LicenseKeyEntry` object with associated type ID and license key.

   ```
   $licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
   $licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
   $licenseKeyEntry.TypeId = "vmware-vsphere"
   $licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
   ```

4. Associate the `LicenseKeys` attribute of the `LicenseData` object you created in step 3 with the `LicenseKeyEntry` object.

   ```
   $licenseData.LicenseKeys += $licenseKeyEntry
   ```

5. Update the license data for the data center with the `LicenseData` object and verify that the license is associated with the host container.

   ```
   $licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData)
   $licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
   ```

6. Provision one or more hosts with vSphere Auto Deploy and assign them to the data center or to the cluster that you assigned the license data to.

7. You can use the vSphere Client to verify that the host is successfully assigned to the default license `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` .

All hosts that you assigned to the data center are now licensed automatically.

Related Links

Prepare Your System for vSphere Auto Deploy on page 1231

Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.

Using vSphere Auto Deploy Cmdlets on page 1232

vSphere Auto Deploy cmdlets are implemented as Microsoft PowerShell cmdlets and included in PowerCLI. Users of vSphere Auto Deploy cmdlets can take advantage of all PowerCLI features.

Reprovisioning Hosts

Use vSphere Auto Deploy to reprovision ESXi hosts with a different image profile or a different host profile.

vSphere Auto Deploy supports multiple reprovisioning options. You can perform a simple reboot or reprovision with a different image profile or a different host profile.

The following reprovisioning operations are available.

- Simple reboot.
- Reboot of hosts for which the user answered questions during the boot operation.
- Reprovision with a different image profile.
- Reprovision with a different host profile.

Reprovision Hosts with Simple Reboot Operations

You can reprovisions ESXi hosts with the image profile, host profile, custom script, and vCenter Server location assigned during first boot.

A simple reboot of a host that is provisioned with vSphere Auto Deploy requires only that all prerequisites are still met. The process uses the previously assigned image profile, host profile, custom script, and vCenter Server location.

- Verify that all associated items like are available. An item can be an image profile, host profile, custom script or vCenter Server inventory location.
- Verify that the host has the identifying information (asset tag, IP address) it had during previous boot operations.

1. Place the host in maintenance mode.

Host Type	Action
Host is part of a DRS cluster	VMware DRS migrates virtual machines to appropriate hosts when you place the host in maintenance mode.
Host is not part of a DRS cluster	You must migrate all virtual machines to different hosts and place each host in maintenance mode.

2. Reboot the host.

The host shuts down. When the host reboots, it uses the image profile that the vSphere Auto Deploy server provides. The vSphere Auto Deploy server also applies the host profile stored on the vCenter Server system.

Reprovision a Host with a New Image Profile by Using PowerCLI

You can use vSphere Auto Deploy to reprovision a host with a new image profile in a PowerCLI session by changing the rule for the host and performing a test and repair compliance operation.

- Verify that the setup you performed during the first boot operation is in place.

Several options for reprovisioning hosts exist.

- If the VIBs that you want to use support live update, you can use an `esxcli software vib` command. In that case, you must also update the rule set to use an image profile that includes the new VIBs.

- During testing, you can apply an image profile to an individual host with the `Apply-EsxImageProfile` cmdlet and reboot the host so the change takes effect. The `Apply-EsxImageProfile` cmdlet updates the association between the host and the image profile but does not install VIBs on the host.
- In all other cases, use this procedure.

1. At the PowerShell prompt, run the `Connect-VIServer`PowerCLI cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Determine the location of a public software depot that contains the image profile that you want to use, or define a custom image profile with vSphere ESXi Image Builder.

3. Run `Add-EsxSoftwareDepot` to add the software depot that contains the image profile to the PowerCLI session.

Depot Type	Cmdlet
Remote depot	Run `Add-EsxSoftwareDepot` *`depot_url`*.
ZIP file	1. Download the ZIP file to a local file path or create a mount point local to the PowerCLI machine. 2. Run `Add-EsxSoftwareDepot C:\`*`file_path\my_offline_depot`*`.zip`.

4. Run `Get-EsxImageProfile` to see a list of image profiles, and decide which profile you want to use.

5. Run `Copy-DeployRule` and specify the `ReplaceItem` parameter to change the rule that assigns an image profile to hosts.

   The following cmdlet replaces the current image profile that the rule assigns to the host with the *`my_new_imageprofile`* profile. After the cmdlet completes, `myrule` assigns the new image profile to hosts. The old version of `myrule` is renamed and hidden.

   ```
   Copy-DeployRule myrule -ReplaceItem my_new_imageprofile
   ```

6. Test the rule compliance for each host that you want to deploy the image to.
   a) Verify that you can access the host for which you want to test rule set compliance.

      ```
      Get-VMHost -Name ESXi_hostname
      ```

   b) Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

      ```
      $tr = Test-DeployRuleSetCompliance ESXi_hostname
      ```

   c) Examine the differences between the contents of the rule set and configuration of the host.

      ```
      $tr.itemlist
      ```

      The system returns a table of current and expected items if the host for which you want to test the new rule set compliance is compliant with the active rule set.

      ```
      CurrentItem                          ExpectedItem
      -----------                          ------------
      my_old_imageprofilemy_new_imageprofile
      ```

   d) Remediate the host to use the revised rule set the next time you boot the host.

      ```
      Repair-DeployRuleSetCompliance $tr
      ```

7. Reboot the host to provision it with the new image profile.

Write a Rule and Assign a Host Profile to Hosts

vSphere Auto Deploy can assign a host profile to one or more ESXi hosts.

The host profile might include information about storage configuration, network configuration, or other characteristics of the host. If you add a host to a cluster, that cluster's host profile is used.

- Install PowerCLI and all prerequisite software. For information, see vCenter Server Installation and Setup.
- Export the host profile that you want to use.

In many cases, you assign a host to a cluster instead of specifying a host profile explicitly. The host uses the host profile of the cluster.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.
2. Using the vSphere Client, set up a host with the settings you want to use and create a host profile from that host.
3. Find the name of the host profile by running `Get-VMhostProfile`PowerCLI cmdlet, passing in the ESXi host from which you create a host profile.
4. At the PowerCLI prompt, define a rule in which host profiles are assigned to hosts with certain attributes, for example a range of IP addresses.

   ```
   New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
    "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   The specified item is assigned to all hosts with the specified attributes. This example specifies a rule named testrule2. The rule assigns the specified host profile *`my_host_profile`* to all hosts with an IP address inside the specified range and with a manufacturer of Acme or Zven.
5. Add the rule to the rule set.

   ```
   Add-DeployRule testrule2
   ```

   By default, the working rule set becomes the active rule set, and any changes to the rule set become active when you add a rule. If you use the `NoActivate` parameter, the working rule set does not become the active rule set.

- Assign a host already provisioned with vSphere Auto Deploy to the new host profile by performing compliance test and repair operations on those hosts. For more information, see Test and Repair Rule Compliance .
- Power on unprovisioned hosts to provision them with the host profile.

Test and Repair Rule Compliance

Test new or modified rules for compliance and repair accordingly, as changes in the vSphere Auto Deploy rule set are not updated automatically.

When you add a rule to the vSphere Auto Deploy rule set or modify one or more rules, hosts are not updated automatically. vSphere Auto Deploy applies the new rules only when you test their rule compliance and perform remediation.

- Prepare your system and install the Auto Deploy Server. For more information, see Prepare Your System for vSphere Auto Deploy.
- Verify that your infrastructure includes one or more ESXi hosts provisioned with vSphere Auto Deploy, and that the host on which you installed PowerCLI can access those ESXi hosts.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect to the vCenter Server system that vSphere Auto Deploy is registered with.

   ```
   Connect-VIServer ipv4_or_ipv6_address
   ```

   The cmdlet might return a server certificate warning. In a production environment, make sure no server certificate warnings result. In a development environment, you can ignore the warning.

2. Use PowerCLI to check which vSphere Auto Deploy rules are currently available.

   ```
   Get-DeployRule
   ```

   The system returns the rules and the associated items and patterns.

3. Modify one of the available rules.

   For example, you can change the image profile and the name of the rule.

   ```
   Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
   ```

   You cannot edit a rule already added to the active rule set. Instead, you can copy the rule and replace the item or pattern you want to change.

4. Verify that you can access the host for which you want to test rule set compliance.

   ```
   Get-VMHost -Name MyEsxi42
   ```

5. Run the cmdlet that tests rule set compliance for the host, and bind the return value to a variable for later use.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

6. Examine the differences between the contents of the rule set and configuration of the host.

   ```
   $tr.itemlist
   ```

   If the host for which you want to test the new rule set compliance is compliant with the active rule set, the system returns a table of current and expected items.

   ```
   CurrentItem                          ExpectedItem
   -----------                          ------------
   My Profile 25MyNewProfile
   ```

7. Remediate the host to use the revised rule set the next time you boot the host.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

If the rule you changed specified the inventory location, the change takes effect when you repair compliance. For all other changes, reboot your host to have vSphere Auto Deploy apply the new rule and to achieve compliance between the rule set and the host.

Collect Logs to Troubleshoot ESXi Hosts

You can collect installation or upgrade log files for ESXi. If an installation or upgrade fails, checking the log files can help you identify the source of the failure.

1. Enter the `vm-support` command in the ESXi Shell or through SSH.
2. Navigate to the `/var/tmp/` directory.
3. Retrieve the log files from the `.tgz` file.

vCenter Server Installation and Setup

vCenter Server Installation and Setup describes how to deploy the VMware vCenter Server® appliance.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

vCenter Server Installation and Setup is for anyone who must install and configure VMware vSphere®. These topics are for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

Introduction to vSphere Installation and Setup

vSphere 7.0 provides various options for installation and setup. To ensure a successful vSphere deployment, you should understand the installation and setup options, and the sequence of tasks.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. vCenter Server lets you pool and manage the resources of multiple hosts.

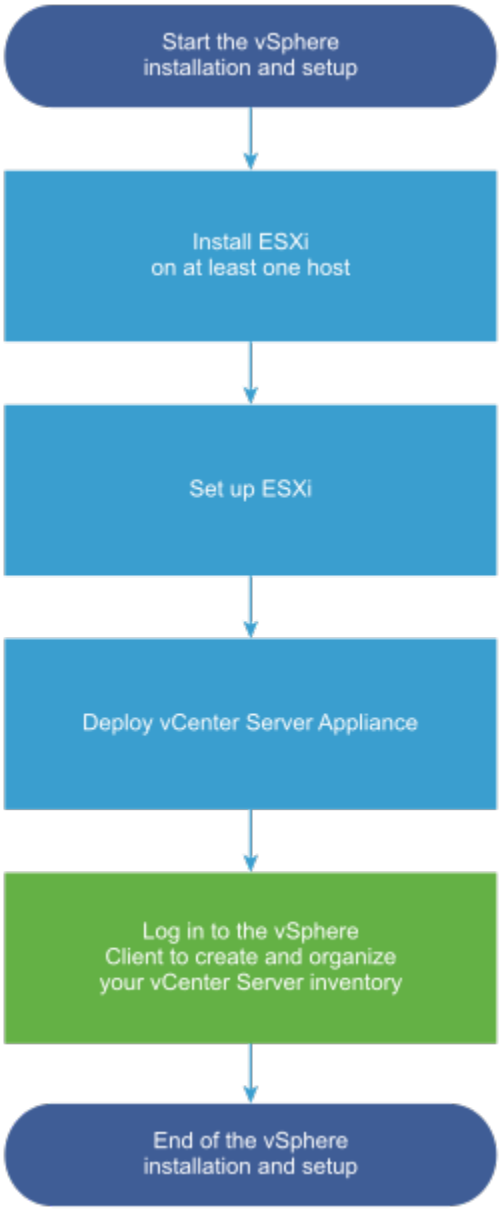
You deploy the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy the vCenter Server appliance on ESXi hosts or on vCenter Server instances.

Overview of the vSphere Installation and Setup Process

vSphere is a sophisticated product with multiple components to install and set up. To ensure a successful vSphere deployment, understand the sequence of tasks required.

Installing vSphere includes the following tasks:

Figure 17: vSphere Installation and Setup Workflow



1. Read the vSphere release notes.
2. Install ESXi.
3. Install vCenter Server.

vCenter Server Components and Services

vCenter Server provides a centralized platform for management, operation, resource provisioning, and performance evaluation of virtual machines and hosts.

The following components are included in the vCenter Server appliance deployments:

- The authentication services contain vCenter Single Sign-On, License service, Lookup Service, and VMware Certificate Authority.

- The vCenter Server group of services contains vCenter Server, vSphere Client, vSphere Auto Deploy, and vSphere ESXi Dump Collector. The vCenter Server appliance also contains the VMware vSphere Lifecycle Manager Extension service and the VMware vCenter Lifecycle Manager.

What Happened to the Platform Services Controller

Beginning in vSphere 7.0, deploying a new vCenter Server or upgrading to vCenter Server 7.0 requires the use of the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server appliance, see the *vSphere Upgrade* documentation.

Authentication Services

vCenter Single Sign-On	The vCenter Single Sign-On authentication service provides secure authentication services to the vSphere software components. By using vCenter Single Sign-On, the vSphere components communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. vCenter Single Sign-On uses vsphere.local as the domain where the vSphere solutions and components are registered during the installation or upgrade process, providing an infrastructure resource. vCenter Single Sign-On can authenticate users from its own internal users and groups, or it can connect to trusted external directory services such as Microsoft Active Directory. Authenticated users can then be assigned registered solution-based permissions or roles within a vSphere environment. vCenter Single Sign-On is required with vCenter Server.
vSphere License Service	The vSphere License service provides common license inventory and management capabilities to all vCenter Server systems within the Single Sign-On domain.
VMware Certificate Authority	VMware Certificate Authority (VMCA) provisions each ESXi host with a signed certificate that has VMCA as the root certificate authority, by default. Provisioning occurs when the ESXi host is added to vCenter Server explicitly or as part of the ESXi host installation process. All ESXi certificates are stored locally on the host.

For information about all authentication services and capabilities, see *vSphere Authentication*.

Services Installed with vCenter Server

These additional components are installed silently when you install vCenter Server. The components cannot be installed separately as they do not have their own installers.

PostgreSQL	A bundled version of the VMware distribution of PostgreSQL database for vSphere and vCloud Hybrid Services.
vSphere Client	The HTML5-based user interface that lets you connect to vCenter Server instances by using a Web browser. This vSphere Client replaces the Flex-based vSphere Web Client in vSphere 7.0.
vSphere ESXi Dump Collector	The vCenter Server support tool. You can configure ESXi to save the VMkernel memory to a network server, rather than to a disk, when the system encounters a critical failure. The vSphere ESXi Dump Collector collects such memory dumps over the network.
vSphere Auto Deploy	The vCenter Server support tool that can provision hundreds of physical hosts with ESXi software. You can specify the image to deploy and the hosts to provision with the image. Optionally, you can specify host profiles to apply to the hosts, and a vCenter Server location (folder or cluster) for each host.
VMware vSphere Lifecycle Manager	vSphere Lifecycle Manager enables centralized, automated patch and version management for VMware vSphere and offers support for VMware ESXi hosts, virtual machines, and virtual appliances.

Overview of the vCenter Server Appliance

The vCenter Server appliance is a preconfigured virtual machine that is optimized for running vCenter Server and the associated services.

The vCenter Server appliance package contains the following software:

- Photon OS® 3.0
- The vSphere authentication services
- PostgreSQL
- VMware vSphere Lifecycle Manager Extension
- VMware vCenter Lifecycle Manager

Version 7.0 of vCenter Server is deployed with virtual hardware version 10, which supports 64 virtual CPUs per virtual machine in ESXi.

During the deployment, you can choose the vCenter Server appliance size for your vSphere environment size and the storage size for your database requirements.

vCenter Server uses the VMware vSphere Lifecycle Manager Extension service. An external vSphere Lifecycle Manager instance on Windows is no longer required for vSphere centralized automated patch and version management. For information about the vCenter Server see vCenter Server Components and Services.

vCenter Server supports high availability. For information about configuring vCenter Server in a vCenter High Availability cluster, see *vSphere Availability*.

vCenter Server supports file-based backup and restore. For information backing up and restoring, see File-Based Backup and Restore of vCenter Server.

For information about the vCenter Server maximums, see VMware Configuration Maximums.

Understanding vSphere Domains and Domain Names

Each vCenter Server is associated with a vCenter Single Sign-On domain. The domain name defaults to vsphere.local, but you can change it during deployment. The domain determines the local authentication space.

vCenter Single Sign-On Domain

When you deploy a vCenter Server appliance, you are prompted to create a vCenter Single Sign-On domain or join an existing domain.

The domain name is used by the VMware Directory Service (vmdir) for all Lightweight Directory Access Protocol (LDAP) internal structuring.

You can give your domain a unique name. To prevent authentication conflicts, use a name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services.

After you specify the name of your domain, you can add users and groups. You can add an Active Directory or LDAP identity source and allow the users and groups in that identity source to authenticate. You can also add vCenter Server instances, or other VMware products, such as vRealize Operations, to the domain.

vCenter Enhanced Linked Mode

vCenter Enhanced Linked Mode allows you to log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Server systems in the group.

You can join up to 15 vCenter Server appliance deployments with vCenter Enhanced Linked Mode in a single vSphere Single Sign-On domain.

You can create a vCenter Enhanced Linked Mode group during the deployment of vCenter Server appliance.

You can also join a vCenter Enhanced Linked Mode group by moving, or repointing, a vCenter Server from one vSphere domain to another existing domain. See Repoint vCenter Server to Another vCenter Server in a Different Domain for information on repointing a vCenter Server node.

vCenter Enhanced Linked Mode for vCenter Server Appliance

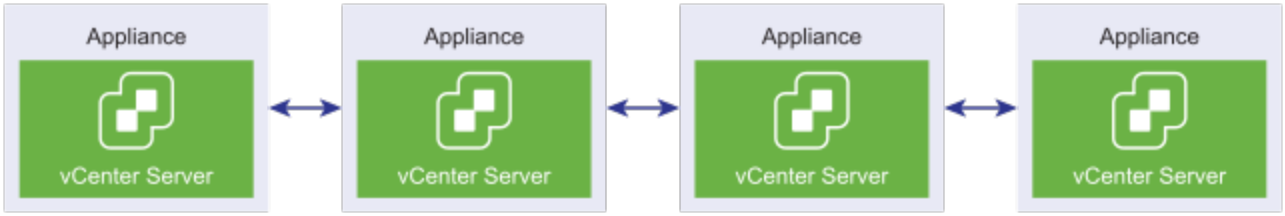
Enhanced linked mode support is enabled for vCenter Server appliance deployments.

You can connect vCenter Server appliance deployments together to form a domain.

Other features include:

- A simplified backup and restore process. See File-Based Backup and Restore of vCenter Server for more information.
- A simplified HA process, removing the need for load balancers.
- Up to 15 vCenter Server appliance deployments can be linked together using enhanced linked mode and displayed in a single inventory view.
- For a vCenter High Availability (vCenter HA) cluster, three nodes are considered one logical vCenter Server node. See "vCenter Architecture Overview" in *vSphere Availability* for the vCenter HA architecture overview. A single vCenter Server standard license is needed for one vCenter HA cluster.

Figure 18: Enhanced Linked Mode for vCenter Server Appliance Deployments



Enhanced Linked Mode with Read Only Replication

If a vCenter High Availability (vCenter HA) instance is connected with another vCenter Server instance with enhanced linked mode and vCenter HA failover occurs to the passive node and is unable to communicate with its replication partner on the other vCenter Server node, the replica on the vCenter HA node enters read-only mode.

Joining a vCenter Enhanced Linked Mode Domain

You can join a vCenter Server appliance to another node during deployment of the vCenter Server appliance.

Note:

You can also join a vCenter Enhanced Linked Mode group by moving, or repointing, a vCenter Server from one vSphere domain to another existing domain. See Repoint vCenter Server to Another vCenter Server in a Different Domain for information on repointing a vCenter Server node.

For example, you can deploy two vCenter Server appliance systems and join the two nodes using vCenter Enhanced Linked Mode.

If you are deploying the vCenter Server appliance nodes with the UI Installer:

1. For Appliance 1, deploy the vCenter Server appliance as an instance on ESXi Host 1. Synchronize the time settings with ESXi Host 1.
2. For Appliance 2, deploy the vCenter Server appliance as an instance on ESXi Host 1 and configure the time settings so that Appliance 2 is synchronized with ESXi Host 1. In stage 2 you select to join the vCenter Single Sign-On server of the deployed appliance on Appliance 1. For specific instructions, see Stage 2 - Set up the Newly Deployed vCenter Server Appliance with an Embedded Platform Services Controller.

If you are deploying the vCenter Server appliance nodes with the CLI:

1. Configure the JSON configuration template `embedded_vCSA_on_VC.json` (or `embedded_vCSA_on_ESXi.json`) for Appliance 1 as an instance on ESXi Host 1. See Prepare Your JSON Configuration File for CLI Deployment for specific instructions on preparing the JSON configuration file.
2. Deploy Appliance 1 by running the `vcsa-cli-installer` command. See Deploy a vCenter Server Appliance by Using the CLI for instructions.
3. Configure the JSON configuration template `embedded_vCSA_replication_on_VC.json` (or `embedded_vCSA_replication_on_ESXi.json`) for Appliance 2 as an instance on ESXi Host 1. Enter the hostname of the first embedded node in the `replication_partner_hostname` field in the `sso` section.
4. Deploy Appliance 2 by running the `vcsa-cli-installer` command using the `embedded_vCSA_replication_on_VC.json` (or `embedded_vCSA_replication_on_ESXi.json`) file.

Deploying the vCenter Server Appliance

You can deploy the vCenter Server appliance to manage your vSphere environment.

You can deploy the vCenter Server appliance on an ESXi host 6.5 or later, or on an ESXi host or DRS cluster from the inventory of a vCenter Server instance 6.5 or later.

For information about the software included in the vCenter Server appliance 7.0, see Overview of the vCenter Server Appliance.

For information about the software and hardware requirements for deploying the vCenter Server appliance, see System Requirements for the vCenter Server Appliance.

The vCenter Server installer contains executable files both for GUI and CLI deployments.

- The GUI deployment is a two stage process. The first stage is a deployment wizard that deploys the OVA file of the appliance on the target ESXi host or vCenter Server instance. After the OVA deployment finishes, you are redirected to the second stage of the process that sets up and starts the services of the newly deployed appliance.
- The CLI deployment method involves running a CLI command against a JSON file that you previously prepared. The CLI installer parses the configuration parameters and their values from the JSON file and generates an OVF Tool command that automatically deploys and sets up the appliance. The CLI deployment automatically runs both stage 1 then stage 2, with no user interaction required.

The vCenter Server appliance has the following default user names:

User Name	Description
root	Use this user name to log in to the appliance operating system and the vCenter Server Management Interface. You set the password while deploying the virtual appliance.
administrator@*your_domain_name*	Use this user name for vCenter Single Sign-On login. You set the password while creating the vCenter Single Sign-On domain. You create a vCenter Single Sign-On domain during the deployment of a vCenter Server appliance in a new vCenter Single Sign-On domain. After you create a vCenter Single Sign-On domain, only the administrator@*your_domain_name* user has the privileges required to log in to vCenter Single Sign-On and vCenter Server. The administrator@*your_domain_name* user can proceed as follows: • Add an identity source in which additional users and groups are defined to vCenter Single Sign-On. • Give permissions to the users and groups. For information about adding identity sources and giving permissions to the users and groups, see *vSphere Authentication* .

For information about upgrading and patching the vCenter Server appliance, see *vSphere Upgrade*.

For information about configuring vCenter Server, see *vCenter Server Configuration*.

If you want to set up vCenter Server to use an IPv6 address version, use the fully qualified domain name (FQDN) or host name of the appliance. To set up an IPv4 address, the best practice is to use the FQDN or host name of the appliance, because the IP address can change if assigned by DHCP.

System Requirements for the vCenter Server Appliance

You can deploy the vCenter Server appliance on an ESXi host 6.5 or later, or on a vCenter Server instance 6.5 or later. Your system must also meet specific software and hardware requirements.

When you use Fully Qualified Domain Names, verify that the client machine from which you are deploying the appliance and the network on which you are deploying the appliance use the same DNS server.

Before you deploy the appliance, synchronize the clocks of the target server and all vCenter Server instances on the vSphere network. Unsynchronized clocks might result in authentication problems and can cause the installation to fail or prevent the appliance services from starting. See Synchronizing Clocks on the vSphere Network.

Hardware Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance, you can select to deploy an appliance that is suitable for the size of your vSphere environment. The option that you select determines the number of CPUs and the amount of memory for the appliance.

Hardware Requirements for the vCenter Server Appliance

The hardware requirements for a vCenter Server appliance depend on the size of your vSphere inventory.

Table 40: Hardware Requirements for a vCenter Server Appliance

	Number of vCPUs	Memory
Tiny environment (up to 10 hosts or 100 virtual machines)	2	12 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	4	19 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	8	28 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	16	37 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	24	56 GB

Note: If you want to add an ESXi host with more than 512 LUNs and 2,048 paths to the vCenter Server inventory, you must deploy a vCenter Server appliance for a large or x-large environment.

Storage Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance, the ESXi host or DRS cluster on which you deploy the appliance must meet minimum storage requirements. The required storage depends not only on the size of the vSphere environment and the storage size, but also on the disk provisioning mode.

Storage Requirements for the vCenter Server Appliance

The storage requirements are different for each vSphere environment size and depend on your database size requirements.

Table 41: Storage Requirements for a vCenter Server Appliance

	Default Storage Size	Large Storage Size	X-Large Storage Size
Tiny environment (up to 10 hosts or 100 virtual machines)	579 GB	1992 GB	4279 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	694 GB	2046 GB	4304 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	908 GB	2140 GB	4468 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	1358 GB	1958 GB	4518 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	2283 GB	2383 GB	4620 GB

Note: The storage requirements include the requirements for the vSphere Lifecycle Manager that runs as a service in the vCenter Server appliance.

Related Links

Determine the Oracle Database Size and the Storage Size for the New Appliance on page 1322

Before upgrading a vCenter Server appliance or migrating a vCenter Server on Windows that uses an external Oracle database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new vCenter Server appliance database using an embedded PostgreSQL database.

Software Requirements for the vCenter Server Appliance

The VMware vCenter Server appliance can be deployed on ESXi 6.5 hosts or later, or on vCenter Server instances 6.5 or later.

You can deploy the vCenter Server appliance using the GUI or CLI installer. You run the installer from a network client machine that you use to connect to the target server and deploy the appliance on the server. You can connect directly to an ESXi 6.5 host on which to deploy the appliance. You can also connect to a vCenter Server 6.5 instance to deploy the appliance on an ESXi host or DRS cluster that resides in the vCenter Server inventory.

For information about the requirements for network client machine, see System Requirements for the vCenter Server Installer.

Required Ports for vCenter Server

The vCenter Server system must be able to send data to every managed host and receive data from the vSphere Client. To enable migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other through predetermined TCP and UDP ports.

vCenter Server is accessed through predetermined TCP and UDP ports. If you manage network components from outside a firewall, you might be required to reconfigure the firewall to allow access on the appropriate ports. For the list of all supported ports and protocols in vSphere, see the VMware Ports and Protocols Tool™ at https://ports.broadcom.com.

During installation, if a port is in use or is blocked using a denylist, the vCenter Server installer displays an error message. You must use another port number to proceed with the installation. There are internal ports that are used only for inter-process communication.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from vCenter Server. If a built-in firewall exists between any of these elements, the installer opens the ports during the installation or upgrade process. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

To configure the vCenter Server system to use a different port to receive vSphere Client data, see the *vCenter Server and Host Management* documentation.

DNS Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance with a static IP address, you ensure that in case of system restart, the IP address of the appliance remains the same.

Before you deploy the vCenter Server appliance with a static IP address, you must verify that this IP address has a valid internal domain name system (DNS) registration.

When you deploy the vCenter Server appliance, the installation of the web server component that supports the vSphere Client fails if the installer cannot look up the fully qualified domain name (FQDN) for the appliance from its IP address. Reverse lookup is implemented using PTR records.

If you plan to use an FQDN for the appliance system name, you must verify that the FQDN is resolvable by a DNS server, by adding foward and reverse DNS A records.

You can use the `nslookup` command to verify that the DNS reverse lookup service returns an FQDN when queried with the IP address and to verify that the FQDN is resolvable.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

If you use DHCP instead of a static IP address for the vCenter Server appliance, verify that the appliance name is updated in the domain name service (DNS). If you can ping the appliance name, the name is updated in DNS.

Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Client instances. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and vSphere Client.

vSphere Client Software Requirements

Use of the vSphere Client requires a supported web browser.

VMware has tested and supports the following guest operating systems and browser versions for the vSphere Client.

Supported Guest Operating Systems	• Windows 32-bit and 64-bit • Mac OS
Supported Browser Versions	• Google Chrome 89 or later • Mozilla Firefox 80 or later • Microsoft Edge 90 or later **Note:** Later versions of these browsers are likely to work, but have not been tested.

Preparing for Deployment of the vCenter Server Appliance

Before you deploy the vCenter Server appliance, you must download the vCenter Server installer ISO file and mount it to a network virtual machine or physical server from which you want to perform the deployment.

The machine from which you deploy the appliance must run on a Windows, Linux, or Mac operating system that meets the operating system requirements. See System Requirements for the vCenter Server Installer.

System Requirements for the vCenter Server Installer

You can run the vCenter Server GUI or CLI installer from a network client machine that is running on a Windows, Linux, or Mac operating system of a supported version.

To ensure optimal performance of the GUI and CLI installers, use a client machine that meets the minimum hardware requirements.

Table 42: System Requirements for the GUI and CLI Installers

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
Windows	• Windows 8, 8.1, 10 • Windows 2012 x64 bit • Windows 2012 R2 x64 bit	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
	• Windows 2016 x64 bit • Windows 2019 x64	
Linux	• SUSE 15 • Ubuntu 16.04 and 18.04	4 GB RAM, 1 CPU having 2 cores with 2.3 GHz, 16 GB hard disk, 1 NIC **Note:** The CLI installer requires 64-bit OS.
Mac	• macOS v10.13, 10.14, 10.15 • macOS High Sierra, Mojave, Catalina	8 GB RAM, 1 CPU having 4 cores with 2.4 GHz, 150 GB hard disk, 1 NIC

Note: For client machines that run on Mac 10.13 or later, concurrent GUI deployments of multiple appliances are unsupported. You must deploy the appliances in a sequence.

Note: Visual C++ redistributable libraries need to be installed to run the CLI installer on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa-cli-installer/win32/vcredist` directory.

Note: Deploying the vCenter Server appliance with the GUI requires a minimum resolution of 1024x768 to properly display. Lower resolutions can truncate the UI elements.

Download and Mount the vCenter Server Installer

VMware releases the vCenter Server appliance ISO image, which contains GUI and CLI installers for the vCenter Server appliance.

- Access to Broadcom Support.
- Verify that your client machine meets the system requirements for the vCenter Server installer. See System Requirements for the vCenter Server Installer.

With the GUI and CLI executable files that are included in the vCenter Server installer, you can:

- Deploy the vCenter Server appliance.
- Upgrade the vCenter Server appliance.
- Converge older versions of vCenter Server with an external Platform Services Controller to the current version of vCenter Server.
- Restore a vCenter Server appliance from a file-based backup.

1. Log in to Broadcom Support Portal.
2. Download the vCenter Server appliance ISO image.

   See the Knowledge Base article.
3. Download the vCenter Server appliance ISO image.
4. Confirm that the md5sum is correct by using an MD5 checksum tool.
5. Mount the ISO image to the client machine from which you want to deploy, upgrade, migrate, or restore the appliance.

   Note: ISO mounting software that does not allow more than eight directory levels, for example, MagicISO Maker on Windows, is unsupported.

   For Linux OS and Mac OS, Archive Manager is unsupported.

   For Mac OS, you can use DiskImageMounter.
   For Ubuntu 14.04, you can use Disk Image Mounter.
   For SUSE 12 OS, you can use the terminal.

   ```
   $ sudo mkdir mount_dir
   ```

```
$ sudo mount -o loop VMware-vCSA-all-version_number-build_number.iso mount_dir
```

Important: Due to a security change in MacOS Catalina, you must modify the security settings on your computer until the vCenter Server deployment completes. If you attempt to run the installer under MacOS Catalina without modifying the security settings, the vCenter Server installer reports the error:`ovftool cannot be opened because the developer cannot be verified.` For more information, see KB 79416.

Open the `readme.txt` file and review the information about the other files and directories in the vCenter Server appliance ISO image.

Synchronizing Clocks on the vSphere Network

Verify that all components on the vSphere network have their clocks synchronized. If the clocks on the physical machines in your vSphere network are not synchronized, SSL certificates and SAML tokens, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server`vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause the first boot of a component in your environment to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server is not synchronized with NTP or PTP. Similarly, issues can arise if the destination vCenter Server migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server instance.

- The target ESXi host where the destination vCenter Server is to be deployed is synchronized to NTP or PTP.
- The ESXi host running the source vCenter Server is synchronized to NTP or PTP.
- When upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, if the vCenter Server appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP or PTP.
- If you are upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, verify that the source vCenter Server or vCenter Server appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the VMware knowledge base article at https://kb.vmware.com/s/article/1318.

To synchronize ESXi clocks with an NTP or a PTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see topic *Edit the Time Configuration of an ESXi Host in the VMware Host Client* in the *vSphere Single Host Management - VMware Host Client* documentation.

To learn how to change time synchronization settings for vCenter Server, see topic *Configure the System Time Zone and Time Synchronization Settings* in the *vCenter Server Configuration* documentation.

To learn how to edit the time configuration for a host by using the vSphere Client, see topic *Editing the Time Configuration Settings of a Host* in the *vCenter Server and Host Management* documentation.

System Clock Synchronization Between the Client and Server

To establish a secure TLS connection to a vCenter Server (the server), the system where you are running the CLI installer (the client) must not have its system clock slower or faster than the server's system clock by an acceptable limit (tolerance).

See Table 43: Client Clock Tolerance for specific values for each deployment scenario.

Note: The client clock values are applicable only for vCenter Server 6.7 and later.

Table 43: Client Clock Tolerance

Deployment Scenario	Clock Tolerance	Connection Notes
Linking one vCenter Server with another vCenter Server	When deploying the second vCenter Server, the clock tolerance for the client and the first vCenter Server must not exceed 10 minutes.	
Installing a vCenter Server appliance using a container vCenter Server with a `*._on_vc.json` template.	The maximum clock tolerance between the client and the container vCenter Server is 8 hours 20 minutes.	

Prerequisites for Deploying the vCenter Server Appliance

To ensure a successful deployment of the vCenter Server appliance, you must perform some required tasks and pre-checks before running the installer.

General Prerequisites

- Download and Mount the vCenter Server Installer.

Target System Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the vCenter Server Appliance.
- If you want to deploy the appliance on an ESXi host, verify that the ESXi host is not in lockdown or maintenance mode and not part of a fully automated DRS cluster.
- If you want to deploy the appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to use NTP servers for time synchronization, verify that the NTP servers are running and that the time between the NTP servers and the target server on which you want to deploy the appliance is synchronized.

vCenter Enhanced Linked Mode Prerequisites

When deploying a new vCenter Server as part of an Enhanced Linked Mode deployment, create an image-based backup of the existing vCenter Server nodes in your environment. You can use the backup as a precaution in case there is a failure during the deployment process.

If the deployment fails, delete the newly deployed vCenter Server appliance, and restore the vCenter Server nodes from their respective image-based backups. You must restore all the nodes in the environment from their image-based backups. Failing to do so can cause the replication partners to be out of synchronization with the restored node.

- To learn more about creating vCenter Enhanced Linked Mode deployments, see vCenter Enhanced Linked Mode.
- To learn about image-based backs, see Image-Based Backup and Restore of a vCenter Server Environment.

Network Prerequisites

If you plan to assign a static IP address and an FQDN as a system name in the network settings of the appliance, verify that you have configured the forward and reverse DNS records for the IP address.

GUI Deployment of the vCenter Server Appliance

You can use the GUI installer to perform an interactive deployment of a vCenter Server appliance.

When you perform the GUI deployment, you download the vCenter Server installer on a network client machine, run the deployment wizard from the client machine, and provide the inputs that are required for the appliance deployment and setup.

The GUI deployment process includes a series of two stages.

Figure 19: Stage 1 - OVA Deployment

The first stage walks you through the deployment wizard to choose the deployment type and appliance settings. This stage completes the deployment of the OVA file on the target server with the deployment type and appliance settings that you provide.

As an alternative to performing the first stage of the deployment with the GUI installer, you can deploy the OVA file of the vCenter Server appliance by using the vSphere Client. After the OVA deployment, you must log in to the vCenter Server Management Interface of the newly deployed appliance to proceed with the second stage of the deployment process. See "Deploy an OVF or OVA Template" in *vSphere Virtual Machine Administration* vSphere Virtual Machine Administration for information about deploying an OVA file using the vSphere Client.

Figure 20: Stage 2 - Appliance Setup

The second stage walks you through the setup wizard to configure the appliance time synchronization and vCenter Single Sign-On. This stage completes the initial setup and starts the services of the newly deployed appliance.

As an alternative to performing the second stage of the deployment with the GUI installer, you can log in to the vCenter Server Management Interface of the newly deployed appliance, https://`FQDN_or_IP_address`:5480.

Required Information for Deploying a vCenter Server Appliance

When you use the GUI method to deploy a vCenter Server appliance, the wizard prompts you for deployment and setup information. It is a best practice to keep a record of the values that you enter in case you must reinstall the product.

You can use this worksheet to record the information that you need for deploying a vCenter Server appliance.

Table 44: Required Information During Stage 1 of the GUI Deployment Process

Required Information	Default	Your Entry
FQDN or IP address of the target server on which you want to deploy the appliance. The target server can be either an ESXi host or a vCenter Server instance.	-	
HTTPS port of the target server	443	
User name with administrative privileges on the target server • If your target server is an ESXi host, use root.	-	

Required Information	Default	Your Entry
• If your target server is a vCenter Server instance, use *user_name*@*your_domain_name*, for example, administrator@vsphere.local.		
Password of the user with administrative privileges on the target server	-	
Data center from the vCenter Server inventory on which you want to deploy the appliance . Target server must be a vCenter Server instance. Optionally you can provide a data center folder.	-	
ESXi host or DRS cluster from the data center inventory on which you want to deploy the appliance	-	
VM name for the appliance • Must not contain a percent sign (%), backslash (\), or forward slash (/) • Must be no more than 80 characters in length	vCenter Server	
Password for the root user of the appliance operating system • Must contain only lower ASCII characters without spaces. • Must be at least 8 characters, but no more than 20 characters in length • Must contain at least one uppercase letter • Must contain at least one lowercase letter • Must contain at least one number • Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!)	-	
Deployment size of the vCenter Server appliance for your vSphere environment. See Hardware Requirements for the vCenter Server Appliance for information about the deployment sizes you can select. The option that you select determines the number of CPUs and the amount of memory for the appliance.	Tiny	
Storage size of the vCenter Server appliance for your vSphere environment. The required storage depends not only on the size of the vSphere environment, but also on the disk provisioning mode. See Storage Requirements for the vCenter Server Appliance. Increase the default storage size if you want larger volume for SEAT data (stats, events, alarms, and tasks).	Default	
Name of the datastore on which you want to store the configuration files and virtual disks of the appliance **Note:** The installer displays a list of datastores that are accessible from your target server.	-	
Enable or disable Thin Disk Mode	Disabled	
Name of the network to which to connect the appliance	-	

Required Information	Default	Your Entry
Note: The installer displays a drop-down menu with networks that depend on the network settings of your target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu. The network must be accessible from the client machine from which you perform the deployment.		
IP version for the appliance address Can be either IPv4 or IPv6.	IPv4	
IP assignment for the appliance address Can be either static or DHCP.	static	
FQDN For a static IP assignment vCenter Server uses FQDN or IP address as the system name.	-	
IP address	-	
For IPv4 networks, you can use either a subnet mask or a network prefix. Subnet mask uses a dot decimal notation (for example, 255.255.255.0). An IPv4 network prefix is an integer between 0 and 32. For IPv6 networks, you must use a network prefix. An IPv6 network prefix is an integer between 0 and 128 .	-	
Default gateway	-	
DNS servers separated by commas	-	
System name (FQDN) Only if you use DHCP with IPv4 and have a Dynamic DNS (DDNS) server available in your environment.	-	

Table 45: Required Information During Stage 2 of the GUI Deployment Process

Required Information	Default	Your Entry
Time synchronization settings You can synchronize the time of the appliance either with the time of the ESXi host or with one or more NTP servers. If you want to use more than one NTP servers, you must provide the IP addresses or FQDNs of the NTP servers as a comma-separated list.	Synchronize time with NTP servers	
Enable or disable SSH access **Note:** vCenter Server High Availability requires remote SSH access to the appliance.	Disabled	
Name for the new vCenter Single Sign-On domain For example, vsphere.local.	-	
Password for the administrator account, administrator@*your_domain_name* • Must be at least 8 characters, but no more than 20 characters in length	-	

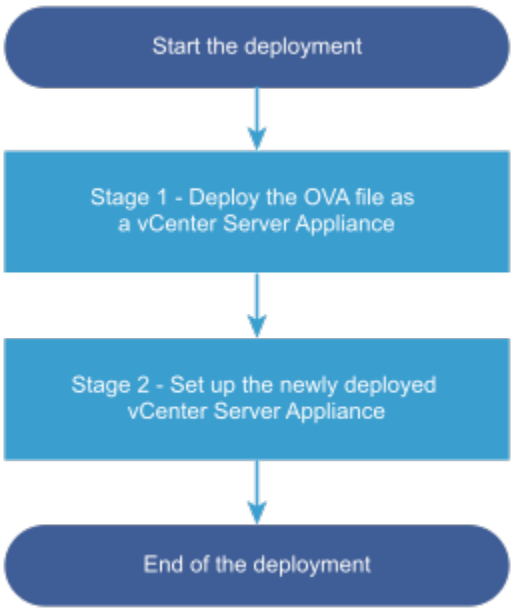
Required Information	Default	Your Entry
• Must contain at least one uppercase letter • Must contain at least one lowercase letter • Must contain at least one number • Must contain at least one special character, such as ampersand (&), hash key (#), and percent sign (%)		
Password of the vCenter Single Sign On administrator user for the domain	-	
Join or do not participate in the VMware Customer Experience Improvement Program (CEIP) For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.	Join the CEIP	

Deploy the vCenter Server Appliance by Using the GUI

You can use the GUI installer to perform an interactive deployment of a vCenter Server appliance. You must run the GUI deployment from a Windows, Linux, or Mac machine that is in the network on which you want to deploy the appliance.

- See Prerequisites for Deploying the vCenter Server Appliance.
- See Required Information for Deploying a vCenter Server Appliance.

Figure 21: Deployment Workflow of a vCenter Server Appliance



Stage 1 - Deploy the OVA File as a vCenter Server Appliance

With stage 1 of the deployment process, you deploy the OVA file, which is included in the vCenter Server installer, as a vCenter Server appliance.

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.

- For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
- For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.

2. On the Home page, click **Install** to start the deployment wizard.
3. Review the Introduction page to understand the deployment process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. Connect to the target server on which you want to deploy the vCenter Server appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the appliance.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target ESXi host, and click **Yes** to accept the certificate thumbprint.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the appliance.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of user with vCenter Single Sign-On administrative privileges on the vCenter Server instance, for example, the administrator@*`your_domain_name`* user. 4. Click **Next**. 5. Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target vCenter Server instance, and click **Yes** to accept the certificate thumbprint. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the appliance, and click **Next** **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the appliance, and click **Next**.

6. On the Set up appliance VM page, enter a name for the vCenter Server appliance, set the password for the root user, and click **Next**.

   The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

   The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

7. Select the deployment size for the vCenter Server appliance for your vSphere inventory.

   See Hardware Requirements for the vCenter Server Appliance for information about the deployment sizes you can select. The option that you select determines the number of CPUs and the amount of memory for the appliance.

8. Select the storage size for the vCenter Server appliance, and click **Next**.

   The required storage depends not only on the size of the vSphere environment, but also on the disk provisioning mode. See Storage Requirements for the vCenter Server Appliance.

9. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.

10. On the Configure network settings page, set up the network settings.

    The IP address or the FQDN of the appliance is used as a system name. It is recommended to use an FQDN. However, if you want to use an IP address, use static IP address allocation for the appliance, because IP addresses allocated by DHCP might change.

Option	Action
Network	Select the network to which to connect the appliance. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu.
IP version	Select the version for the appliance IP address. You can select either IPv4 or IPv6.
IP assignment	Select how to allocate the IP address of the appliance. • **static** The wizard prompts you to enter the IP address and network settings. • **DHCP** A DHCP server is used to allocate the IP address. Select this option only if a DHCP server is available in your environment. If there is an enabled DDNS in your environment, you can enter a preferred fully qualified domain name (FQDN) for the appliance.
Common Ports	You can customize the HTTP and HTTPS ports (optional). If specifying a custom HTTP and HTTPS port number, ensure that you do not use a port number already in use by vCenter Server, or the default HTTP and HTTPS ports of 80 and 443.

11. On the Ready to complete stage 1 page, review the deployment settings for the vCenter Server appliance and click **Finish** to start the OVA deployment process.

12. Wait for the OVA deployment to finish, and click **Continue** to proceed with stage 2 of the deployment process to set up and start the services of the newly deployed appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface to set up and start the services.

The newly deployed vCenter Server appliance is running on the target server but the services are not started.

Stage 2 - Set up the Newly Deployed vCenter Server Appliance with an Embedded Platform Services Controller

When the OVA deployment finishes, you are redirected to stage 2 of the deployment process to set up and start the services of the newly deployed vCenter Server Appliance with an embedded Platform Services Controller.

1. Review the introduction to stage 2 of the deployment process and click **Next**.
2. Configure the time settings in the appliance, optionally enable remote SSH access to the appliance, and click **Next**.

Option	Description
Synchronize time with the ESXi host	Enables periodic time synchronization, and VMware Tools sets the time of the guest operating system to be the same as the time of the ESXi host.
Synchronize time with NTP servers	Uses a Network Time Protocol server for synchronizing the time. If you select this option, you must enter the names or IP addresses of the NTP servers separated by commas.

3. Create a new vCenter Single Sign-On domain or join an existing domain.

Option	Description
Create a new Single Sign-On domain	Creates a new vCenter Single Sign-On domain. 1. Enter the domain name, for example `vsphere.local`. **Note:** Ensure that the domain name does not contain any upper-case letters. 2. Set the password for the vCenter Single Sign-On administrator account. This is the password for the user administrator@*`your_domain_name`*. 3. Confirm the administrator password, and click **Next**.
Join an existing vCenter Single Sign-On domain	Joins a new vCenter Single Sign-On server to an existing vCenter Single Sign-On domain. You must provide the information about the vCenter Single Sign-On server to which you join the new vCenter Single Sign-On server. 1. Enter the fully qualified domain name (FQDN) or IP address of the vCenter Single Sign-On server to join. 2. Enter the HTTPS port to use for communication with the vCenter Single Sign-On server. 3. Enter the domain name for the vCenter Single Sign-On you are joining, for example `vsphere.local`. 4. Enter the password of the vCenter Single Sign-On administrator account. 5. Click **Next**.

   When you select to join an existing vCenter Single Sign-On domain, you enable the Enhanced Linked Mode feature. The infrastructure data is replicated with the joined vCenter Single Sign-On server.

4. Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

   For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

5. On the Ready to complete page, review the configuration settings for the vCenter Server appliance, click **Finish**, and click **OK** to complete stage 2 of the deployment process and set up the appliance.
6. Optional: After the initial setup finishes, enter the URL from the browser with **https://*vcenter_server_appliance_fqdn*/ui** to go to the vSphere Client and log in to the vCenter Server instance in the vCenter Server appliance, or click the **https://*vcenter_server_appliance_fqdn*:443** to go the vCenter Server appliance Getting Started page.
7. Click **Close** to exit the wizard.

   You are redirected to the vCenter Server appliance Getting Started page.

You can configure high availability for the vCenter Server appliance. For information about providing vCenter Server appliance high availability, see *vSphere Availability*.

CLI Deployment of the vCenter Server Appliance

You can use the CLI installer to perform a silent deployment of a vCenter Server appliance on an ESXi host or vCenter Server instance.

The CLI deployment process includes downloading the vCenter Server installer on a network virtual machine or physical server from which you want to perform the deployment, preparing a JSON configuration file with the deployment information, and running the deployment command.

You can also watch the video about how to install the vCenter Server appliance by using the CLI installer.

Prepare Your JSON Configuration File for CLI Deployment

Before you run the CLI installer to deploy a vCenter Server appliance, you must prepare a JSON file with configuration parameters and their values for your deployment specification.

- You must be familiar with the JSON syntax.
- Download and Mount the vCenter Server Installer.

The vCenter Server installer contains JSON templates for all deployment options. For information about the templates, see JSON Templates for CLI Deployment of the vCenter Server Appliance.

You can deploy an appliance with minimum configurations by setting values to the configuration parameters in the JSON template for your specification. You can edit the preset values, remove configuration parameters, and add configuration parameters for custom configurations.

For a complete list of the configuration parameters and their descriptions, navigate to the installer subdirectory for your operating system and run the `vcsa-deploy install --template-help` command or see Deployment Configuration Parameters.

1. In the vCenter Server installer, navigate to the `vcsa-cli-installer` directory, and open the `templates` subfolder.
2. Copy the deployment templates from the `install` subfolder to your workspace.

   Important: The path to the JSON configuration files must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.
3. In a text editor, open the template file for your specification.

   To ensure the correct syntax of your JSON configuration file, use a JSON editor.

4. Fill in the values for the required configuration parameters and, optionally, enter additional parameters and their values.
   For example, if you want to use an IPv4 DHCP assignment for the network of the appliance, in the `network` subsection of the template, change the value of the `mode` parameter to `dhcp` and remove the default configuration parameters that are for a static assignment.

   ```
   "network": {
       "ip_family": "ipv4",
       "mode": "dhcp"
   },
   ```

   Important:

   The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

   To set a value that contains a backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-7.0.0.`*`XXXX-YYYYYYY`*`_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.`*`XXXX-YYYYYYY`*`_OVF10.ova`.

   The Boolean values must contain only lowercase characters, that is, a value can be either `true` or `false` . For example, `"ssh_enable":false` .
5. Optional: Use a JSON editor of your choice to validate the JSON file.
6. Save in UTF-8 format and close the file.

You can create and save additional templates if needed for your deployment specification.

JSON Templates for CLI Deployment of the vCenter Server Appliance

The vCenter Server installer includes JSON templates with the minimum configuration parameters for all deployment options. The templates are located in the `vcsa-cli-installer/templates/install` directory.

For each deployment option, there is one template for deploying the appliance on an ESXi host and another template for deploying the appliance on a vCenter Server instance.

Table 46: Deployment JSON Templates Included in the vCenter Server Installer

Template	Description
`embedded_vCSA_on_ESXi.json`	Contains the minimum configuration parameters required for the deployment of a vCenter Server appliance on an ESXi host.
`vCSA_with_cluster_on_ESXi.json`	Contains the minimum configuration parameters required for the deployment of a vCenter Server appliance with a single node vSAN and a vLCM managed cluster on an ESXi host.
`embedded_vCSA_on_VC.json`	Contains the minimum configuration parameters required for the deployment of a vCenter Server appliance on a vCenter Server instance.
`embedded_vCSA_replication_on_ESXi.json`	Contains the minimum configuration parameters required for the deployment of a vCenter Server appliance as a replication partner to another embedded vCenter Server on an ESXi host.

Template	Description
embedded_vCSA_replication_on_VC.json	Contains the minimum configuration parameters required for the deployment of a vCenter Server appliance replication partner to another vCenter Server appliance on a vCenter Server instance.

Deployment Configuration Parameters

When you prepare your JSON configuration files for a CLI deployment, you must set parameters and values to provide input data for the deployment of a vCenter Server appliance.

Sections and Subsections of Configuration Parameters in the JSON Deployment Files

The configuration parameters in the JSON configuration files for a CLI upgrade are organized in sections and subsections.

Table 47: Sections and Subsections of Configuration Parameters in the JSON Deployment Files

Section	Subsection	Description
new_vcsa - describes the appliance you want to deploy	esxi	Use only if you want to deploy the appliance directly on an ESXi host. Contains the configuration parameters that describe the target ESXi host. Depending on whether you want to configure a vSAN or a vLCM Managed Cluster during the deployment, see the relevant section for a detailed information about the configuration parameters. • Table 48: Configuration Parameters in the new_vcsa Section, esxi Subsection for Deployments with a vSAN and a vLCM Managed Cluster • #unique_437/unique_437_Connect_42_TABLE_636C07CD-1750-4887-9F0E-F3D09933B683-en **Note:** You must fill in either the esxi or the vc subsection.
	vc	Use only if you want to deploy the appliance on the inventory of a vCenter Server instance. Contains the configuration parameters that describe the target ESXi host or DRS cluster from the vCenter Server inventory. See Table 50: Configuration Parameters in the new_vcsa Section, vc Subsection. **Note:** You must fill in either the vc or the esxi subsection.
	appliance	Contains the configuration parameters that describe the appliance. See Table 51: Configuration Parameters in the new_vcsa Section, appliance Subsection.
	network	Contains the configuration parameters that describe the network settings for the appliance. See Table 52: Configuration Parameters in the new_vcsa Section, network Subsection.
	os	Contains the configuration parameters that describe the operating system settings for the appliance. See Table 53: Configuration Parameters in the new_vcsa Section, os Subsection.
	sso	Contains the configuration parameters that describe the vCenter Single Sign-On settings for the appliance. See Table 54: Configuration Parameters in the new_vcsa Section, sso Subsection.
	ovftool_arguments	Optional subsection for adding arbitrary arguments and their values to the OVF Tool command that the installer generates.

Section	Subsection	Description
		Important: The vCenter Server installer does not validate the configuration parameters in the `ovftool_arguments` subsection. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
`ceip` - describes joining the VMware Customer Experience Improvement Program (CEIP)	`settings`	Contains only the `ceip_enabled` configuration parameter to join or not to join the VMware Customer Experience Improvement Program (CEIP). See Table 55: Configuration Parameters in the ceip Section, settings Subsection. **Note:** If set to `true` , you must run the CLI deployment command with the `--acknowledge-ceip` argument. For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

Important:

The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To set a value that contains a backslash (\) or a quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password. Similarly, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYYY_OVF10.ova`.

Boolean values must contain only lowercase characters. It must be either `true` or `false` . For example, `"ssh_enable":false` .

Configuration Parameters in the `new_vcsa` Section

Table 48: Configuration Parameters in the `new_vcsa` Section, `esxi` Subsection for Deployments with a vSAN and a vLCM Managed Cluster

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target ESXi host on which you want to deploy the appliance.
`username`	string	A user name with administrative privileges on the target ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the target ESXi host.
`deployment_network`	string	The name of the network to which to connect the appliance. **Note:** The network must be accessible from the target ESXi host. Ignored if the target ESXi host has only one network.
`datacenter`	string	A specific data center you want to create.
`cluster`	string	The name of the vSAN or vLCM managed cluster.
`compression_only`	Boolean	Set the value to `true` to enable compression on the vSAN cluster. If this parameter is set to `true` , the `deduplication_and_compression` parameter must be set to`false` .
`deduplication_and_compression`	Boolean	Set the value to `true` to enable compression and deduplication on the vSAN cluster. If this parameter is set to `true` , the `compression_only` parameter must be set to `false` .
`cache_disk`		A list of UUIDs or canonical names of disks you want to use for cache. Specify only SSDs.

Name	Type	Description
capacity_disk		A list of UUIDs or canonical names of disks you want to use for storage. Specify either SSDs or HDDs.
enable_vlcm	Boolean	Set to true to create a vLCM managed cluster.
datastore	string	The name of the datastore where you want to store the configuration files and virtual disks of the appliance. **Note:** The datastore must be accessible from the ESXi host. If you are using the thin disk mode, the datastore size should have a miniumu of 25GB space.
port	integer	The HTTPS reverse proxy port of the target ESXi host. The default port is 443. Use only if the target ESXi host uses a custom HTTPS reverse proxy port.

Table 49: Configuration Parameters in the `new_vcsa` Section, `esxi` Subsection for Deployments without a vSAN or a vLCM Managed Cluster

Name	Type	Description
hostname	string	The IP address or FQDN of the target ESXi host on which you want to deploy the appliance.
username	string	A user name with administrative privileges on the target ESXi host, for example, root.
password	string	The password of the user with administrative privileges on the target ESXi host.
deployment_network	string	The name of the network to which to connect the appliance. **Note:** The network must be accessible from the target ESXi host. Ignored if the target ESXi host has only one network.
datastore	string	The name of the datastore where you want to store the configuration files and virtual disks of the appliance. **Note:** The datastore must be accessible from the ESXi host. If you are using the thin disk mode, the datastore size should have a miniumu of 25GB space.
port	integer	The HTTPS reverse proxy port of the target ESXi host. The default port is 443. Use only if the target ESXi host uses a custom HTTPS reverse proxy port.

Table 50: Configuration Parameters in the `new_vcsa` Section, `vc` Subsection

Name	Type	Description
hostname	string	The IP address or FQDN of the target vCenter Server instance on which you want to deploy the appliance.
username	string	vCenter Single Sign-On administrator user name on the target vCenter Server instance, for example, administrator@vsphere.local.
password	string	The password of the vCenter Single Sign-On administrator user on the target vCenter Server instance.

Name	Type	Description
deployment_network	string	The name of the network to which to connect the appliance. **Note:** The network must be accessible from the target ESXi host or DRS cluster on which you want to deploy the appliance. Ignored if the target ESXi host or DRS cluster has only one network.
datacenter	array	The vCenter Server datacenter that contains the target ESXi host or DRS cluster on which you want to deploy the appliance. If the datacenter is located in a folder or a structure of folders, specify the value as a comma-separated list of strings. For example, `["parent_folder", "child_folder", "datacenter_name"]` **Note:** The value is case-sensitive.
datastore	string	The name of the datastore that you want to store the configuration files and virtual disks of the appliance. **Note:** The datastore must be accessible from the target ESXi host or DRS cluster. The datastore must have at least 25 GB of free space.
port	integer	The HTTPS reverse proxy port of the target vCenter Server instance. The default port is 443. Use only if the target vCenter Server instance uses a custom HTTPS reverse proxy port.

target	array	The target ESXi host or DRS cluster on which you want to deploy the appliance.
		Important: You must provide the name that is displayed in the vCenter Server inventory. For example, if the name of the target ESXi host is an IP address in the vCenter Server inventory, you cannot provide an FQDN.
		If the target ESXi host or DRS cluster is located in a folder or a structure of folders, specify the value as a comma-separated list of strings. For example,
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		If the target ESXi host is part of a cluster, specify the path as a comma-separated list of strings. For example,
		`["cluster_name", "esxi-host.domain.com"]`
		Note: The value is case-sensitive.

vm_folder	string	Optional. The name of the VM folder where the appliance is deployed.

Table 51: Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection

Name	Type	Description
thin_disk_mode	Boolean	Set to `true` to deploy the appliance with thin virtual disks.
deployment_option	string	The size of the appliance. • Set to `tiny` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 12 GB of memory, and 315 GB of storage. • Set to `tiny-lstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 12 GB of memory, and 1390 GB of storage. • Set to `tiny-xlstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 12 GB of memory, and 3145 GB of storage.

Name	Type	Description
		• Set to `small` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 19 GB of memory, and 380 GB of storage. • Set to `small-lstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 19 GB of memory, and 1435 GB of storage. • Set to `small-xlstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 19 GB of memory, and 3195 GB of storage. • Set to `medium` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 28 GB of memory, and 600 GB of storage. • Set to `medium-lstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 28 GB of memory, and 1600 GB of storage. • Set to `medium-xlstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 28 GB of memory, and 3360 GB of storage. • Set to `large` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 37 GB of memory, and 965 GB of storage. • Set to `large-lstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the large storage size. Deploys an appliance with 16 CPUs, 37 GB of memory, and 1665 GB of storage. • Set to `large-xlstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 37 GB of memory, and 3425 GB of storage. • Set to `xlarge` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 24 CPUs, 56 GB of memory, and 1705 GB of storage. • Set to `xlarge-lstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 24 CPUs, 56 GB of memory, and 1805 GB of storage. • Set to `xlarge-xlstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 24 CPUs, 56 GB of memory, and 3565 GB of storage.
`image`	string	Optional. A local file path or URL to the vCenter Server appliance installation package. By default the installer uses the installation package that is included in the ISO file, in the `vcsa` folder.
`name`	string	The VM name for the appliance. Must contain only ASCII characters except a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
`ovftool_path`	string	Optional. A local file path to the OVF Tool executable file. By default the installer uses the OVF Tool instance that is included in the ISO file, in the `vcsa/ovftool` folder.

Table 52: Configuration Parameters in the `new_vcsa` Section, `network` Subsection

Name	Type	Description
`ip_family`	string	IP version for the network of the appliance.

Name	Type	Description
		Set to `ipv4` or `ipv6` .
`mode`	string	IP assignment for the network of the appliance. Set to `static` or `dhcp` .
`ip`	string	IP address for the appliance. Required only if you use static assignment, that is, if you set the `mode` parameter to `static` . You must set an IPv4 or IPv6 address that corresponds to the network IP version, that is, to the value of the `ip.family` parameter. An IPv4 address must comply with the RFC 790 guidelines. An IPv6 address must comply with the RFC 2373 guidelines.

`dns_servers`	string or array	IP addresses of one or more DNS servers.
		To set more than one DNS server, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["x.y.z.a", "x.y.z.b"]`
		or
		`"x.y.z.a, x.y.z.b"`
		Optional when the `mode` parameter is set to `static` . Not supported when mode is set to `DHCP` .

`prefix`	string	Network prefix length. Use only if the `mode` parameter is set to `static` . Remove if the `mode` parameter is set to `dhcp` . The network prefix length is the number of bits that are set in the subnet mask. For example, if the subnet mask is 255.255.255.0, there are 24 bits in the binary version of the prefix length, so the network prefix length is 24. For IPv4 version, the value must be between `0` and `32` . For IPv6 version, the value must be between `0` and `128` .
`gateway`	string	IP address of the default gateway. For IPv6 version, the value can be `default` .
`ports`	string	Optional. Port numbers that the vCenter Server appliance uses for direct HTTP connections. By default, port 80 redirects requests to HTTPS port 443. You can customize the vCenter Server HTTP and HTTPS ports. If specifying a custom HTTP and HTTPS port number, ensure that you do not use a port already in use by vCenter Server, or the default HTTP and HTTPS ports of 80 and 443. The options to specify a custom port are: `"rhttpproxy.ext.port1":"`*`port_number`*`"` for the HTTP port, and `"rhttpproxy.ext.port2:"`*`port_number`*`"` for the HTTPS port. The following example specifies ports 81 and 444 for the HTTP and HTTPS ports: `ports: {"rhttpproxy.ext.port1":"81", "rhttpproxy.ext.port2":"444"}` For more information on ports in use by vCenter Server, see Required Ports for vCenter Server .
`system_name`	string	Primary network identity. Can be an IP address or FQDN, preferably FQDN. You cannot change the value of this parameter after the deployment. The FQDN and dotted-decimal numbers must comply with the RFC 1123 guidelines.

Table 53: Configuration Parameters in the `new_vcsa` Section, `os` Subsection

Name	Type	Description
`password`	string	The password for the root user of the appliance operating system.

Name	Type	Description
		The password must contain between 8 and 20 characters, at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!). All characters must be lower ASCII characters without spaces.

`ntp_servers`	string or array	Optional. Host names or IP addresses of one or more NTP servers for time synchronization.
		To set more than one NTP server, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["x.y.z.a", "x.y.z.b"]`
		or
		`"x.y.z.a, x.y.z.b"`

`ssh_enable`	Boolean	Set to `true` to enable SSH administrator login to the appliance. **Note:** vCenter Server appliance high availability requires remote SSH access to the appliance.
`time_tools_sync`	Boolean	Optional. Set to `true` to deploy the appliance with the VMware Tools time synchronization. VMware Tools synchronizes the time of the appliance with the time of the ESxi host. Ignored if you set NTP servers for time synchronization, that is, if you set the `ntp.servers` parameter.

Table 54: Configuration Parameters in the `new_vcsa` Section, `sso` Subsection

Name	Type	Description
`password`	string	Password of the vCenter Single Sign-On administrator user, administrator@*`your_domain_name`*. If you are deploying a vCenter Server appliance as the first instance in a new vCenter Single Sign-On domain, you must set the password for the vCenter Single Sign-On administrator user. The password must contain between 8 and 20 characters, at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!). All characters must be ASCII characters.
`domain_name`	string	vCenter Single Sign-On domain name, for example, vsphere.local. If you are deploying a vCenter Server appliance as the first instance in a new vCenter Single Sign-On domain, you must set the name for the new vCenter Single Sign-On domain.
`replication_partner_hostname`	string	The system name of the partner vCenter Server. Required only if you are deploying a replication partner in an existing vCenter Single Sign-On domain.
`first_instance`	string	Set `first_instance` to `true` if you do not want to set the replication partner for this node. If you want to set the replication partner for this node, set `first_instance` to `false` and provide the value of the `replication_partner_hostname` as the FQDN of a previously converged node which is currently in an embedded vCenter Server topology.
`sso_port`	integer	The HTTPS reverse proxy port of the partner vCenter Server . The default port is 443. Use only if the partner uses a custom HTTPS reverse proxy port.

Configuration Parameters in the `ceip` Section

Table 55: Configuration Parameters in the `ceip` Section, `settings` Subsection

Name	Type	Description
`ceip_enabled`	Boolean	Set to `true` to join the CEIP for this appliance.

Syntax of the CLI Deployment Command

You can use command arguments to set the execution parameters of the deployment command.

You can add a space-separated list of arguments to the CLI deployment command.

```
vcsa-deploy install path_to_the_json_filelist_of_arguments
```

Argument	Description
`--accept-eula`	Accepts the end-user license agreement. Required for executing the deployment command.
`--acknowledge-ceip`	Confirms your acknowledgement of your VMware Customer Experience Improvement Program (CEIP) participation. Required if the `ceip.enabled` parameter is set to `true` in the JSON deployment template.
`-v`, `--verbose`	Adds debug information to the console output.
`-t`, `--terse`	Hides the console output. Displays only warning and error messages.
`--log-dir`*`LOG_DIR`*	Sets the location of the log and other output files.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters in the JSON file and deploys the appliance. Does not perform verification of the OVF Tool parameters.
`--no-esx-ssl-verify`	Skips the SSL verification for ESXi connections. **Important:** Avoid using this option because it might cause problems during deployment or after deployment because of not validated identity of the target ESXi host.
`--no-ssl-certificate-verification`	Skips security certificate verification for all server connections.
`--operation-id`*`OPERATION_ID`*	Provides an operation ID to track installation activities.
`--pause-on-warnings`	Pauses and waits for acknowledgment of warnings.
`--verify-template-only`	Performs basic template verification of the configuration parameters in the JSON file. Does not deploy the appliance.
`--precheck-only`	Performs only the basic template verification and OVF Tool parameter verification. Does not deploy the appliance.
`--sso-ssl-thumbprint`*`SSL-SHA1-THUMBPRINT`*	Validates server certificate against the supplied SHA1 thumbprint.
`-h`, `--help`	Displays the help message for the `vcsa-deploy install` command.
`--template-help`	Displays the help message for the use of configuration parameters in the JSON deployment file.

After the execution finishes, you can get the exit code of the command.

Exit Code	Description
0	Command ran successfully
1	Runtime error
2	Validation error
3	Template error

Deploy a vCenter Server Appliance by Using the CLI

You can use the CLI installer to perform an unattended deployment of a vCenter Server appliance. You must run the CLI deployment from a Windows, Linux, or Mac machine that is in the network on which you want to deploy the appliance.

- See Prerequisites for Deploying the vCenter Server Appliance.
- Prepare Your JSON Configuration File for CLI Deployment.
- Review Syntax of the CLI Deployment Command.
- Verify that the user name with which you are logged in to your client machine, the path to the vCenter Server installer, the path to your JSON configuration file, and the string values in your JSON configuration file contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.
- The Visual C++ redistributable libraries version 14.0 or newer needs to be installed to run this utility on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa\ovftool\win32\vcredist` directory.

1. Navigate to the `vcsa-cli-installer` subdirectory for your operating system.
   - If you are running the deployment on Windows OS, navigate to the `vcsa-cli-installer\win32` directory.
   - If you are running the deployment on Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.
   - If you are running the deployment on Mac OS, navigate to the `vcsa-cli-installer/mac` directory.
2. Optional: Run a pre-deployment check without deploying the appliance to verify that you prepared the deployment template correctly.

   ```
   vcsa-deploy install --precheck-only path_to_the_json_file
   ```

3. Run the deployment command.

   ```
   vcsa-deploy install --accept-eula --acknowledge-ceip optional_argumentspath_to_the_json_file
   ```

   Use *optional_arguments* to enter space-separated arguments to set additional execution parameters of the deployment command.

   For example, you can set the location of the log and other output files that the installer generates.

   ```
   vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_locationpath_to_the_json_file
   ```

Deploy Multiple vCenter Server Appliances Using the CLI

You can deploy multiple instances vCenter Server appliances concurrently (in batch mode) using the CLI installer.

To deploy multiple instances concurrently, create JSON templates for all the vCenter Server instances in your deployment. The CLI installer assesses the topology of the deployment using the JSON templates, and determines the order. For this reason, the JSON templates must use static IP addresses for all vCenter Server instances in the deployment that are dependant upon one another.

Important: The JSON templates you create for each appliance must use a static IP address to resolve the network addresses of other appliances in the deployment upon which they have a dependency.

To perform the batch deployment, place the JSON templates defining your deployment in a single directory. When invoked, the CLI installer deploys your existing deployment using the topology defined in the JSON templates.

1. In your workspace, create a folder to contain the JSON files for batch deployment. For example, *MyWorkspace*/BatchDeploy.
2. Prepare each JSON configuration file and copy the file to your batch deployment folder. See Prepare Your JSON Configuration File for CLI Deployment for instructions on configuring the JSON files.
3. Navigate to the vcsa-cli-installer subdirectory for your operating system.
   - If you are running the deployment on Windows OS, navigate to the vcsa-cli-installer\win32 directory.
   - If you are running the deployment on Linux OS, navigate to the vcsa-cli-installer/lin64 directory.
   - If you are running the deployment on Mac OS, navigate to the vcsa-cli-installer/mac directory.
4. Optional: Run a pre-deployment check without deploying the appliance to verify that you prepared the deployment template correctly. For example:

   ```
   vcsa-deploy install --precheck-only MyWorkspace/BatchDeploy
   ```

5. Run the deployment command. For example,

   ```
   vcsa-deploy install --accept-eula --acknowledge-ceip optional_argumentsMyWorkspace/BatchDeploy
   ```

   Use *optional_arguments* to enter space-separated arguments to set additional execution parameters of the deployment command.

   For example, you can set the location of the log and other output files that the installer generates.

   ```
   vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_locationMyWorkspace/BatchDeploy
   ```

File-Based Backup and Restore of vCenter Server

vCenter Server supports a file-based backup and restore mechanism that helps you to recover your environment after failures.

You can use the vCenter Server Interface to create a file-based backup of the vCenter Server. After you create the backup, you can restore it by using the GUI installer of the appliance.

You use the vCenter Server Interface to perform a file-based backup of the vCenter Server core configuration, inventory, and historical data of your choice. The backed-up data is streamed over FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB to a remote system. The backup is not stored on the vCenter Server.

You can perform a file-based restore only for a vCenter Server that you have previously backed up by using the vCenter Server Interface. You can perform such restore operation by using the GUI installer of the vCenter Server appliance. The process consists of deploying a new vCenter Server appliance and copying the data from the file-based backup to the new appliance.

Important: If you back up a vCenter Server High Availability cluster, the backup operation only backs up the primary vCenter Server instance. Before restoring a vCenter Server High Availability cluster, you must power off the active, passive, and witness nodes. The restore operation restores the vCenter Server in non- vCenter Server High Availability mode. You must reconstruct the cluster after the restore operation completes successfully.

Considerations and Limitations for File-Based Backup and Restore

When you backup or restore a vCenter Server environment, take into account these considerations and limitations.

Protocols

The following considerations apply to file-based backup and restore protocols:

- FTP and HTTP are not secure protocols.

- Backup servers must support minimum of 10 simultaneous connections for each vCenter Server.
- You can use an FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB server that is up and running with sufficient disk space to store the backup.
- You must have write permissions for upload and read permissions for download.
- Only explicit mode is supported for FTPS.
- If you use HTTP or HTTPS, you must enable WebDAV on the backup Web server.
- You can use only FTP, FTPS, HTTP, or HTTPS to transmit data through an HTTP proxy server.
- You can use IPv4 and IPv6 URLs in file-based backup and restore of a vCenter Server. Mixed mode of IP versions between the backup server and the vCenter Server is unsupported.

Configuration

After a restore, the following configurations revert to the state when the backup was taken.

- Virtual machine resource settings
- Resource pool hierarchy and setting
- Cluster-host membership
- DRS configuration and rules

Storage DRS

If the configuration changes, the following might change after a restore.

- Datastore Cluster configuration
- Datastore Cluster membership
- Datastore I/O Resource Management (Storage I/O Control) settings
- Datastore-Datacenter membership
- Host-Datastore membership

Distributed Power Management

If you put a host into standby mode after a backup, the vCenter Server might force the host to exit standby mode when you restore to the backup.

Distributed Virtual Switch

If you use a distributed virtual switch, you are advised to export separately the distributed virtual switch configuration before you restore to a backup. You can import the configuration after the restore. If you omit this consideration, you may lose the changes made to a distributed virtual switch after the backup. For detailed steps, see the VMware knowledge base article at http://kb.vmware.com/kb/2034602.

Content Libraries

If you delete libraries or items after a backup, you cannot access or use these libraries or items after the restore. You can only delete such libraries or items. A warning message notifies you that there are missing files or folders in the storage backup.

If you create new items or item files after the backup, the Content Library Service has no record of the new items or files after the restore operation. A warning notifies you that extra folders or files were found on the storage backup.

If you create new libraries after the backup, the Content Library Service has no record of the new libraries after restore. The library content exists on the storage backing, but no warning is displayed. You must manually clean the new libraries.

Virtual Machine Life Cycle Operations

- Restoring vCenter Server from a backup that was taken during in-flight relocation operations in the vCenter Server instance.

  After you restore vCenter Server, the vCenter Server view of the virtual machines might be out of sync with the ESXi view of the virtual machines. This is also true if you performed the backup during in-flight operations on vCenter Server. If virtual machines disappear after you restore vCenter Server, you can refer to the following cases.

  a. The missing virtual machine is located on the destination ESXi host and is registered with the destination ESXi host, but it is either an orphan or not in the vCenter Server inventory. You must manually add the virtual machine to the vCenter Server inventory.
  b. The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host and it is not in the vCenter Server inventory. You must manually register the virtual machine to the ESXi host and add the virtual machine back to the vCenter Server inventory.
  c. The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host. In the vCenter Server instance, the missing virtual machine is marked as orphaned. You must remove the virtual machine from the vCenter Server inventory and add it again.
- Restoring vCenter Server from a backup that has an out-of-date linked clone virtual machine layout.

  If you create a linked clone virtual machine after the backup and you restore vCenter Server from the old backup, then after the restore, the vCenter Server does not know about the new linked clone virtual machine until vCenter Server discovers the new linked clone virtual machine. If you remove all existing virtual machines before the new linked clone virtual machine is discovered, then the removal of existing virtual machines corrupts the new linked clone due to missing disks. To avoid this, you must wait until all linked clone virtual machines are discovered by the vCenter Server before you remove virtual machines.
- Restoring vCenter Server from a backup that was taken during virtual machine registration.

  If you are registering a virtual machine during the backup and you restore vCenter Server from the old backup, then after the restore, the virtual machine is marked as orphaned in the vCenter Server instance. You must manually add the virtual machine to the vCenter Server inventory.

vCenter Enhanced Linked Mode

To restore a vCenter Server that is part of an Enhanced Linked Mode, you must have at least one running vCenter Server that has the VMware Directory Service database.

For example, if you have an Enhanced Link Mode deployment with three vCenter Server instances and all three instances are lost due to database corruption, you cannot restore the vCenter Server instances from a file-based backup and restore as at least one running VMware Directory Service database is required to reconcile the restored vCenter Server.

vSphere High Availability

Restoring vCenter Server from a backup might cause it to rollback to older version for the vSphere HA cluster state (HostList, ClusterConfiguration, VM protection state) while the hosts in the cluster have the latest version for the cluster state. You need to make sure the vSphere HA cluster state stays the same during restore and backup operations. Otherwise, the following problems might occur.

- If hosts are added or removed to or from the vSphere HA cluster after backup and before vCenter Server restore, virtual machines could potentially failover to hosts not being managed by the vCenter Server but are still part of the HA cluster.
- Protection state for new virtual machines is not updated on the vSphere HA agents on the hosts that are part of the vSphere HA cluster. As a result, virtual machines are not protected or unprotected.
- New cluster configuration state is not updated on the vSphere HA agents on the hosts that are part of the vSphere HA cluster.

vCenter High Availability

Restoring vCenter Server requires vCenter HA to be reconfigured.

Storage Policy Based Management

Restoring vCenter Server from a backup can lead to the following inconsistencies related to storage policies, storage providers, and virtual machines.

- Registered storage providers after backup are lost.
- Unregistered storage providers after backup re-appear and might show different provider status.
- Changes, such as create, delete, or update, performed on storage policies after backup are lost.
- Changes, such as create, delete, or update, performed on storage policy components after backup are lost.
- Default policy configuration changes for datastores performed after backup are lost.
- Changes in the storage policy association of the virtual machine and its disks, and in their policy compliance might occur.

Virtual Storage Area Network

Restoring vCenter Server from a backup might cause inconsistencies in the vSAN. For information on how to check vSAN health, see *Administering VMware vSAN*.

Patching

Restoring vCenter Server from a backup might result in missing security patches. You must apply them again after the restore is complete. For information on patching the vCenter Server, see *vSphere Upgrade*.

Schedule a File-Based Backup

You can schedule file-based backups for vSphere 6.7 and later. You can set up a schedule that is used to perform periodic backups.

- You must have a FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB server up and running with sufficient disk space to store the backup.

The schedule can be set up with information about the backup location, recurrence, and retention for the backups.

You can only set up one schedule at a time.

1. In a Web browser, go to the vCenter Server Management Interface, https://*`appliance-IP-address-or-FQDN`*:5480.
2. Log in as root.
3. In the vCenter Server Management Interface, click **Backup**.
4. Click **Configure** to set up a backup schedule.
5. Enter the backup location details.

Option	Description
Backup location	Enter the backup location, including the protocol to use to connect to your backup server, the port, the server address, and backup folder to store the backup files. Use one of the following protocols: FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB. For FTP, FTPS, HTTP, or HTTPS the path is relative to the home directory configured for the service.

Option	Description
Backup server credentials	Enter a user name and password of a user with **write** privileges on the backup server.

6. Set the schedule recurrence and time for the backup.

   The recurrence can be set daily, weekly, or you can customize the schedule to run the backup on a specific day or days of the week. You can specify the time of day to run the backup. The default time is 11:59pm.

7. Optional: Enter an Encryption Password if you want to encrypt your backup file.

   If you select to encrypt the backup data, you must use the encryption password for the restore procedure.

8. Select **Retain all backups** or enter the number of backups to retain.

   The retention information provides the number of backups to retain for a given vCenter Server.

   Note: This policy applies to both manual and scheduled backups.

9. Optional: Select **Stats, Events, and Tasks** to back up additional historical data from the database.

10. Click **Create**.

    The backup schedule information is populated in the Backup page.

The complete and in progress backups are listed under Activity.
You can perform an immediate backup with the existing schedule information by selecting **Use backup location and user name from backup schedule** from the backup schedule on the Backup Now dialog box.

Manually Back up vCenter Server by Using the vCenter Server Management Interface

You can use the vCenter Server Management Interface to back up the vCenter Server instance. You can select whether to include historical data, such as stats, events, and tasks, in the backup file.

- You must have an FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB server up and running with sufficient disk space to store the backup.

Note: The backup operation for a vCenter High Availability cluster, backs up only the active node.

1. In a Web browser, go to the vCenter Server Management Interface, https://*`appliance-IP-address-or-FQDN`*:5480.
2. Log in as root.
3. In the vCenter Server Management Interface, click **Backup**.

   The table under Activity displays the most current backup version taken of the vCenter Server.

4. Click **Backup Now**.

   The **Backup Appliance** wizard opens.

5. Optional: Select **Use backup location and user name from backup schedule** to use the information from a scheduled backup.
6. Enter the backup location details.

Option	Description
Backup location	Enter the backup location, including the protocol to use to connect to your backup server, the port, the server address, and backup folder to store the backup files. Use one of the following protocols: FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB.

Option	Description
	For FTP, FTPS, HTTP, or HTTPS the path is relative to the home directory configured for the service.
Backup server credentials	Enter a user name and password of a user with **write** privileges on the backup server. **Note:** Username and password should only contain ASCII characters.

7. Optional: Enter an Encryption Password if you want to encrypt your backup file.
   If you select to encrypt the backup data, you must use the encryption password for the restore procedure.
8. Optional: Select **Stats, Events, and Tasks** to back up additional historical data from the database.
9. Optional: In the **Description** text box, enter a description of the backup.
10. Click **Start** to begin the backup process.

The complete and in progress backups are listed under Activity.

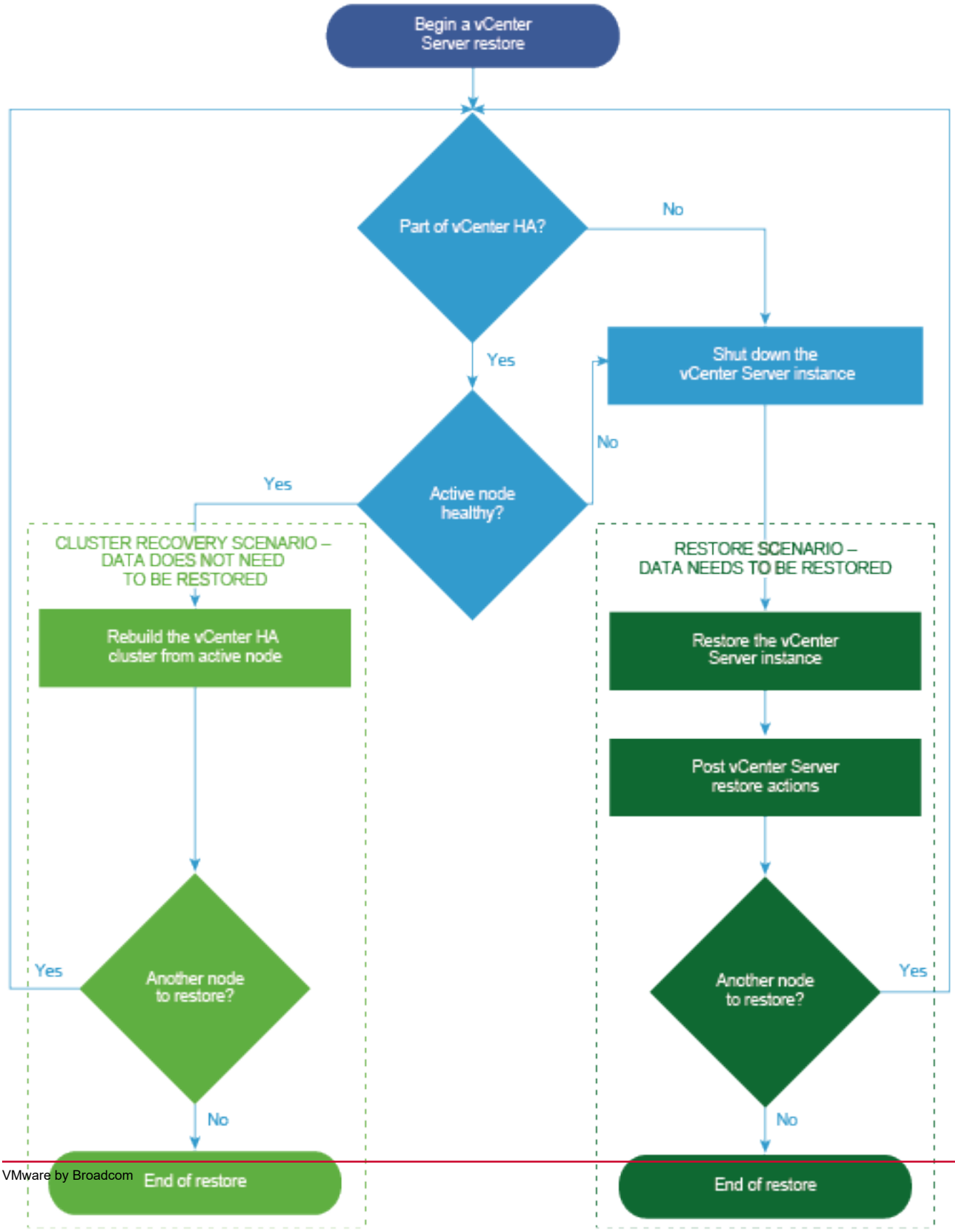
Restore vCenter Server from a File-Based Backup

You can use the vCenter Server appliance GUI installer to restore a vCenter Server to an ESXi host or a vCenter Server instance. The restore procedure has two stages. The first stage deploys a new vCenter Server appliance. The second stage populates the newly deployed vCenter Server appliance with the data stored in the file-based backup.

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the vCenter Server Appliance.

- If the vCenter Server instance is part of a vCenter High Availability cluster, you must power off the active, passive, and witness nodes of the cluster before restoring the vCenter Server.

Figure 22: vCenter Server Restore Workflow



Stage 1 - Deploy a New Appliance

In stage 1 of the restore process, you deploy the OVA file, which is included in the vCenter Server GUI installer.

- Download and mount the vCenter Server installer. See Download and Mount the vCenter Server Installer.
  Note: If you are restoring a backup from a product that has a vCenter Server product patch applied, you must download the full ISO of that particular patch. See Download VMware vSphere.
- If you plan to restore the vCenter Server on an ESXi host, verify that the target ESXi host is not in lockdown or maintenance mode or part of a fully-automated DRS cluster.
- If you plan to restore the vCenter Server on a DRS cluster of a vCenter Server inventory, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to assign a static IP address to the appliance, verify that you have configured the forward and reverse DNS records for the IP address.
- If you are attempting to restore a vCenter Server instance that is still running, power off the backed up vCenter Server before you start the restore operation.

As an alternative to performing the first stage of the restore with the GUI installer, you can deploy the OVA file of the new vCenter Server appliance by using the vSphere Client. After the OVA deployment, you must log in to the vCenter Server Management Interface of the newly deployed appliance to proceed with the second stage of the restore process. See "Deploy an OVF or OVA Template" in *vSphere Virtual Machine Administration* vSphere Virtual Machine Administration for information about deploying an OVA file using the vSphere Client.

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Restore**.
3. Review the Introduction page to understand the restore process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. On the Enter backup details page, enter the details of the backup file that you want to restore, and click **Next**.

Option	Description
Backup location	Enter the server address and backup folder where the backup files are stored. You can also enter the IP address or hostname of the backup server and browse for the location of the backup folder. Specify the protocol to use to retrieve the backup from your backup server. You can select FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB. For example, `ftp://<server_IP_address>/tmp/vCenter/hostname_v-center.com/<backup_filename>`
User name	Enter the user name of a user with **read** privileges on the backup server.
Password	Enter the password of the user with **read** privileges on the backup server.

6. Review the backup information, and click **Next**.
7. Connect to the ESXi host or vCenter Server on which you want to deploy the vCenter Server appliance to use for the restore operation.

Option	Steps
You can connect to an ESXi host on which to deploy the appliance to use for the restore operation.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target ESXi host, and click **Yes** to accept the certificate thumbprint.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the appliance to use for the restore operation.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of user with vCenter Single Sign-On administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4. Click **Next**. 5. Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target vCenter Server instance, and click **Yes** to accept the certificate thumbprint. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the appliance, and click **Next**. **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the appliance, and click **Next**.

8. Accept the certificate warning.
9. Enter a name for the vCenter Server appliance, set up the password for the root user, and click **Next**.
10. Select the deployment size for the new vCenter Server appliance depending on the size of your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory.

Deployment Size Option	Description
	Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

11. Select the storage size for the new vCenter Server appliance, and click **Next**.

    Important: You must consider the storage size of the appliance that you are restoring.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

12. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**.
13. On the Configure network settings page review the settings populated from the backup file of the vCenter Server.
14. Optional: Edit the network configuration to match the current network environment where the vCenter Server is restored.
15. On the Ready to complete stage 1 page, review the deployment settings for the restored vCenter Server appliance and click **Finish** to start the OVA deployment process.
16. Wait for the OVA deployment to finish, and click **Continue** to proceed with stage 2 of the restore process to transfer the data to the newly deployed appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface to transfer the data.

The newly deployed vCenter Server appliance is running on the target server but the data is not copied from the backup location.

Stage 2 - Transfer Data to the Newly Deployed Appliance

After the OVA deployment finishes, you are redirected to stage 2 of the restore process in which the data from the backup location is copied to the newly deployed vCenter Server appliance.

1. Review the introduction to stage 2 of the restore process and click **Next**.
2. Review the backup details and click **Next**.
3. If you are restoring a node with enhanced linked mode support for vCenter Server appliance, you are asked to provide the Single Sign-On credentials. Enter the Single Sign-On user name and password, then click **Validate and Recover**.
4. On the Ready to complete page, review the details, click **Finish**, and click **OK** to complete stage 2 of the restore process.

   The restore process restarts the vCenter Server Management Service. You cannot access the vCenter Server Management API during the restart.

   Important: If a restore operation of a vCenter Server appliance VM results with a failure, you must power off and delete the partially restored VM. After that you can try to restore the VM again.
5. Optional: After the restore process finishes, click the **https://*vcenter_server_appliance_fqdn*/ui** to go to the vSphere Client and log in to the vCenter Server instance , or click the **https://*vcenter_server_appliance_fqdn*:443** to go to the vCenter Server Getting Started page.
6. Click **Close** to exit the wizard.

   You are redirected to the vCenter Server Getting Started page.
7. If the backed up vCenter node is part of a vCenter High Availability cluster, the last needs to be reconfigured after the restore operation completes successfully.

   For information about how to perform backup and restore operations, see *vSphere Availability*.

After successful completion of the restore operation, in the event of a total loss of all storage and servers where all the physical hardware or the data in the hardware is lost, follow the instructions in the VMware knowledge base article at http://kb.vmware.com/kb/76585 in order to recover the system to a pre-restore state at the time of the backup.

Image-Based Backup and Restore of a vCenter Server Environment

You can use vSphere APIs with a third-party product to back up and restore a virtual machine that contains vCenter Server.

You can perform a full image backup of a virtual machine that contains vCenter Server. The virtual machine must use a fully qualified domain name (FQDN) with correct DNS resolution, or the hostname must be configured to be an IP address.

Considerations and Limitations for Image-Based Backup and Restore

When you restore a vCenter Server environment, take into account these considerations and limitations.

Note: Restoring a vCenter Server instance with DHCP network configuration results in changing its IP address. The changed IP address prevents some vCenter Server services from starting properly. To start all vCenter Server services successfully, after the restore, you must reconfigure the IP address of the restored vCenter Server instance to the IP address that the instance was set to when you performed the backup.

Synchronizing Clocks with NTP Time Synchronization Prior to Backup

Before creating a backup of your vCenter Server deployment, verify that all components on the vSphere network have their clocks synchronized using NTP time synchronization. See Synchronizing Clocks on the vSphere Network.

Configuration

After a restore, the following configurations revert to the state when the backup was taken.

- Virtual machine resource settings
- Resource pool hierarchy and setting
- Cluster-host membership
- DRS configuration and rules

Storage DRS

If the configuration changes, the following might change after a restore.

- Datastore Cluster configuration
- Datastore Cluster membership
- Datastore I/O Resource Management (Storage I/O Control) settings
- Datastore-Datacenter membership
- Host-Datastore membership

Distributed Power Management

If you put a host into standby mode after a backup, the vCenter Server might force the host to exit standby mode when you restore to the backup.

Distributed Virtual Switch

If you use a distributed virtual switch, you are advised to export separately the distributed virtual switch configuration before you restore to a backup. You can import the configuration after the restore. If you omit this consideration, you may lose the changes made to a distributed virtual switch after the backup. For detailed steps, see the VMware Knowledge Base article at http://kb.vmware.com/kb/2034602.

Content Libraries

If you delete libraries or items after a backup, you cannot access or use these libraries or items after the restore. You can only delete such libraries or items. A warning message notifies you that there are missing files or folders in the storage backup.

If you create new items or item files after the backup, the Content Library Service has no record of the new items or files after the restore operation. A warning notifies you that extra folders or files were found on the storage backup.

If you create new libraries after the backup, the Content Library Service has no record of the new libraries after restore. The library content exists on the storage backing, but no warning is displayed. You must manually clean the new libraries.

Virtual Machine Life Cycle Operations

- Restoring vCenter Server from a backup that was taken while there are in-flight relocation operations within the vCenter Server instance.

  After you restore vCenter Server, the vCenter Server view of the virtual machines may be out of sync with the ESXi view of the virtual machines. This is also true if you performed the backup while there were in-flight operations on vCenter Server. If virtual machines disappear after you restore vCenter Server, you can refer to the following cases.

  a. The missing virtual machine is located on the destination ESXi host and is registered with the destination ESXi host, but it is not in the vCenter Server inventory. You must manually add the virtual machine to the vCenter Server inventory.
  b. The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host and it is not in the vCenter Server inventory. You must manually register the virtual machine to the ESXi and add the virtual machine back to the vCenter Server inventory.
  c. The missing virtual machine is located on the destination ESXi host, but it is not registered with the destination ESXi host. Within the vCenter Server instance, the missing virtual machine is marked as orphaned. You must remove the virtual machine from the vCenter Server inventory and add it again.
- Restoring vCenter Server from a backup that has an out of date linked clone virtual machine layout.

  If you create a linked clone virtual machine after the backup and you restore vCenter Server from the old backup, then after the restore, vCenter Server does not know about the new linked clone virtual machine until vCenter Server discovers the new linked clone virtual machine. If you remove all existing virtual machines before the new linked clone virtual machine is discovered, then the removal of existing virtual machines corrupts the new linked clone due to missing disks. To avoid this corruption, you must wait until all linked clone virtual machines get discovered by the vCenter Server before you remove virtual machines.

vSphere High Availability

Restoring vCenter Server from a backup may cause it to roll back to older version for the vSphere HA cluster state (HostList, ClusterConfiguration, VM protection state) while the hosts in the cluster have the latest version for the cluster state. Ensure that the vSphere HA cluster state stays the same during restore and backup operations. Otherwise, the following potential problems are present.

- If hosts are added or removed to/from the vSphere HA cluster after backup and before vCenter Server restore, virtual machines could potentially fail over to hosts not managed by the vCenter Server but are still part of the HA cluster.
- Protection states for new virtual machines are not updated on the vSphere HA agents on the hosts which are part of the vSphere HA cluster. As a result, virtual machines are not protected/unprotected.
- New cluster configuration state is not updated on the vSphere HA agents on the hosts which are part of the vSphere HA cluster.

vCenter High Availability

Restoring vCenter Server requires vCenter HA to be reconfigured.

Storage Policy Based Management

Restoring vCenter Server from a backup can lead to the following inconsistencies related to storage policies, storage providers, and virtual machines.

- Registered storage providers after backup are lost.
- Unregistered storage providers after backup reappear and might show different provider status.
- Changes, such as create, delete, or update, performed on storage policies after backup are lost.
- Changes, such as create, delete, or update, performed on storage policy components after backup are lost.
- Default policy configuration changes for datastores performed after backup are lost.

- Changes in the storage policy association of the virtual machine and its disks, and in their policy compliance might occur.

Virtual Storage Area Network

Restoring vCenter Server from a backup may cause inconsistencies in the vSAN. For information how to check vSAN health, see *Administering VMware vSAN*.

Patching

Restoring vCenter Server from a backup might result in missing security patches. You must apply them again after the restore is complete. For information on patching the vCenter Server appliance, see *vSphere Upgrade*.

Restore a vCenter Server Image-based Environment

You can use a third-party product that uses vSphere APIs to restore a virtual machine that contains vCenter Server.

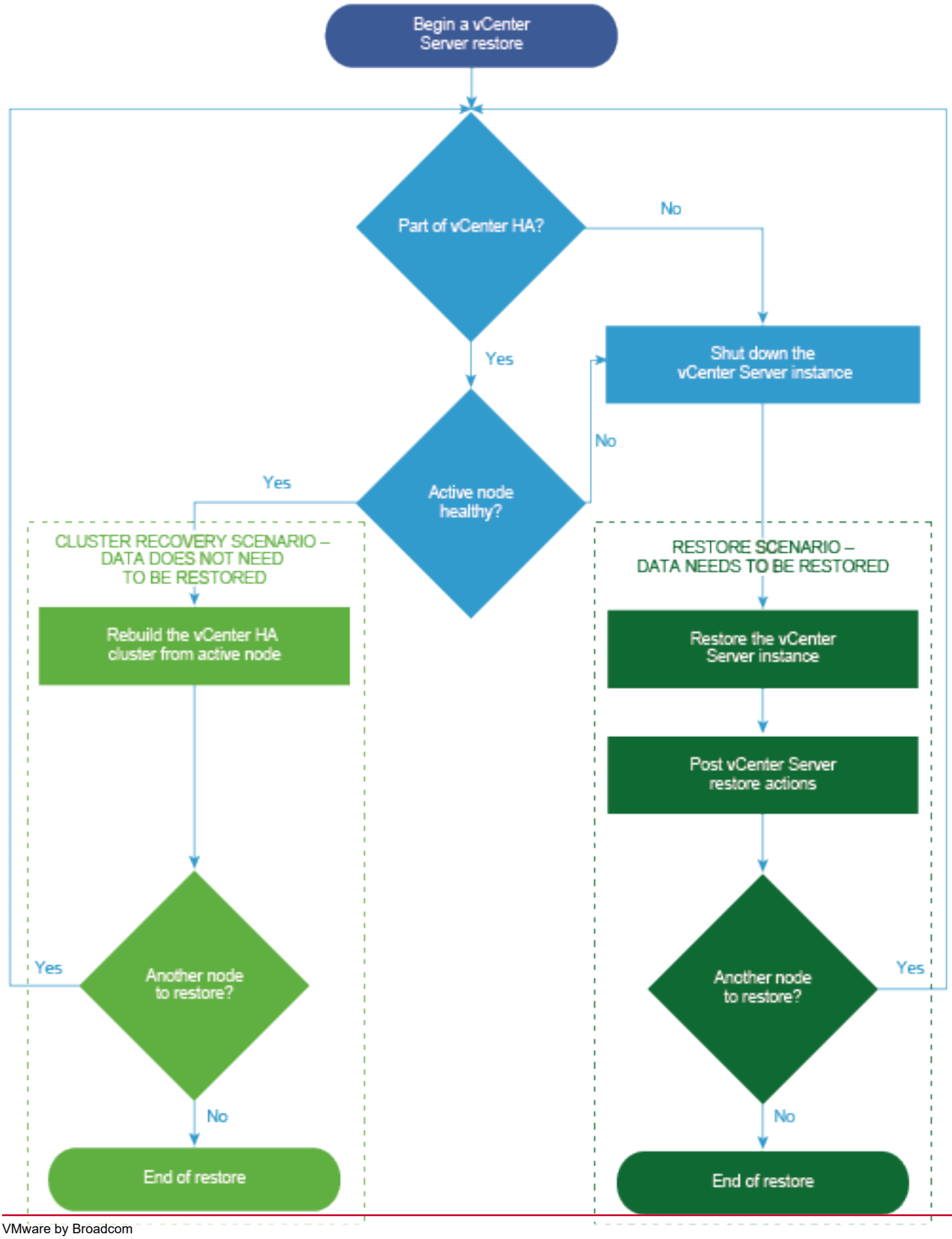
You can perform an image-based restore of a virtual machine that contains vCenter Server. The virtual machine must use a fully qualified domain name (FQDN) with correct DNS resolution, or the host name of the machine must be configured to be an IP address.

You can restore a virtual machine to the original location by either overwriting the backed up virtual machine or by creating a new virtual machine that contains the restored vCenter Server on the same ESXi host. You can also restore the virtual machine on a new ESXi host.

You can restore a virtual machine that contains vCenter Server directly on the ESXi host that is running the third-party appliance when the vCenter Server service becomes unavailable or when you cannot access the third-party user interface by using the vSphere Client.

Important: Restoring virtual machines that have snapshots or that are configured with Fault Tolerance is unsupported.

Figure 23: vCenter Server Restore Workflow



Restore a vCenter Server Instance

You can use a third-party product to restore a vCenter Server environment.

Important: You can back up and restore only virtual machines that contain vCenter Server instances. You cannot back up and restore physical machines that are running vCenter Server by using a third-party product.

1. Restore the vCenter Server virtual machine onto the ESXi host using a third-party solution.
2. Use the `service-control --status --all` command to verify that the services have started.
   Wait for all the vCenter Server services to start, which can take several minutes.
3. Launch the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.
4. When you launch the vCenter Server Management Interface, based on the change in the vCenter Server appliance data you will see one of the following:
   a) If there is a change in the vCenter Server appliance data that needs to be synchronized, reconciliation window will be displayed. Follow the prompts to complete the reconcilation and then provide the Single Sign-On credentials to log into the vCenter Server Management Interface.
   b) If there is no change in the vCenter Server appliance data, the vCenter Server Management Interface login screen will be displayed.

Power on the restored virtual machine that contains the restored vCenter Server instance.

Restore a vCenter Enhanced Linked Mode Environment

You can restore a vCenter Enhanced Linked Mode environment using a third-party solution.

Important: You can back up and restore only virtual machines that contain vCenter Server instances. You cannot back up and restore physical machines that are running vCenter Server by using a third-party product.

1. Restore the vCenter Server virtual machine onto the ESXi host using a third-party solution.
   The services are masked and are not yet running.
2. Use the `systemctl status applmgmt` command to verify that the `systemd` instance of the `applmgmt` service has started.
   Wait for all the vCenter Server services to start, which can take several minutes.
3. Log into the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.

Power on the restored virtual machine that contains the restored vCenter Server instance.

After You Deploy the vCenter Server Appliance

After you deploy the vCenter Server appliance, consider these post installation options before adding inventory for the vCenter Server to manage.

For information about configuring the vSphere Authentication Proxy service, see *vSphere Security*.

For information about upgrading vCenter Server, see *vCenter Server Upgrade*.

Log In to vCenter Server by Using the vSphere Client

You can use the vSphere Client to log in to vCenter Server and manage your vSphere inventory.

The vSphere Client is automatically installed as part of the vCenter Server appliance deployment. This way, the vSphere Client always points to the same vCenter Single Sign-On instance.

1. Open a Web browser and enter the URL for your vCenter Server instance:
   `https://vcenter_server_ip_address_or_fqdn`
   As an alternative, you can open a Web browser and enter the URL for the vSphere Client:
   `https://vcenter_server_ip_address_or_fqdn/ui`.
2. If a warning message about a potential security risk appears, select to continue to the website.

Browser	Action
Microsoft Edge	1. Click **Details**. 2. Under the additional message that appears, click **Go on to the webpage**.
Mozilla Firefox	1. Click **Advanced**. 2. Under the additional message that appears, click **Accept the Risk and Continue**.
Google Chrome	1. Click **Advanced**. 2. Under the additional message that appears, click **Proceed to *vcenter_server_ip_address_or_fqdn***.

3. On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.
4. If the warning message about a potential security risk appears again, repeat Step 2.
5. Enter the credentials of a user who has permissions on vCenter Server and click **Login**.

The vSphere Client connects to all the vCenter Server systems on which the specified user has permissions, and you can view and manage the vSphere inventory.

Repoint vCenter Server to Another vCenter Server in a Different Domain

You can move a vCenter Server from one vSphere domain to another vSphere domain. Services such as tagging and licensing are retained and migrated to the new domain.

The following use cases are supported:

- You can migrate a vCenter Server from an existing domain to an another existing domain with or without replication. The migrated vCenter Server moves from its current Single Sign-On domain and joins the other existing domain as another vCenter Server connected via enhanced linked mode.
  - See Repoint a Single vCenter Server Node to an Existing Domain without a Replication Partner for instructions on repointing a single embedded node from one domain to an existing domain without a replication partner.
  - See Repoint a vCenter Server Node to an Existing Domain with a Replication Partner for instructions on repointing an embedded node from one domain to an existing domain using replication.
- You can migrate a vCenter Server from an existing domain to a newly created domain (where the migrated vCenter Server is the first instance). See Repoint a vCenter Server Node to a New Domain for instructions of this type of repointing. In this case, there is no replication partner.

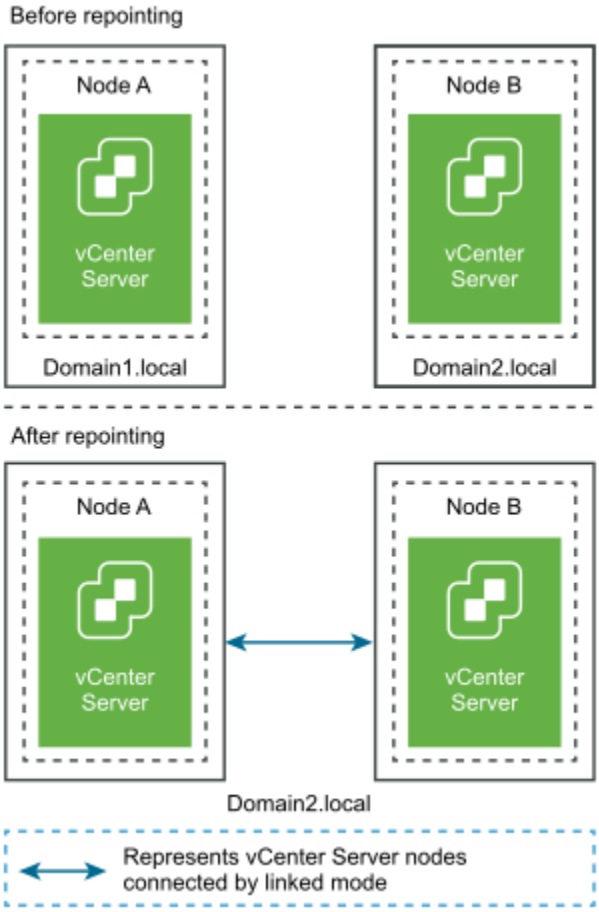
Repoint a Single vCenter Server Node to an Existing Domain without a Replication Partner

You can repoint a single vCenter Server from one Single Sign-On domain to an existing Single Sign-On domain without a replication partner. Each Single Sign-On domain contains a single vCenter Server.

- Repointing is only supported with vCenter Server 6.7 Update 1 and later.
- You must repoint to a vCenter Server that is of the same version and nodes that are of the same version and build number.
- To ensure no loss of data, take a file-based backup of each node before proceeding with repointing the vCenter Server.

See Figure 24: Repointing a Single vCenter Server from One Domain to an Existing Domain for an example of repointing a single vCenter Server from one domain to another existing domain. This is one of many ways to create an Enhanced Linked Mode node. In this case, there is no replication.

Figure 24: Repointing a Single vCenter Server from One Domain to an Existing Domain



1. Make sure that both vCenter Server nodes are powered on before beginning the repointing process.
2. Optional: Run the pre-check mode command. The pre-check mode fetches the tagging (tags and categories) and authorization (roles and privileges) data from the vCenter Server. Pre-check does not migrate any data, but checks for conflicts between the source and destination vCenter Server. For example, run the pre-check with the following CLI:

   ```
   cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
   ```

   Note: Pre-check is not required if a replication partner does not exist (repointing to a newly created domain).

   See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

   The pre-check writes the conflicts to the `/storage/domain-data` directory.
3. Optional: Review the conflicts and apply resolutions for all conflicts, or apply a separate resolution for each conflict.

   The conflict resolutions are:

   - Copy: Create a duplicate copy of the data in the target domain.
   - Skip: Skips copying the data in the target domain.
   - Merge: Merges the conflict without creating duplicates.

   Note: The default resolution mode for Tags and Authorization conflicts is Copy, unless overridden in the conflict files generated during pre-check.

4. Run the `execute` command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain. For example, repointing without a replication partner, run the `execute` command with the following:

   ```
   cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
   ```

   See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

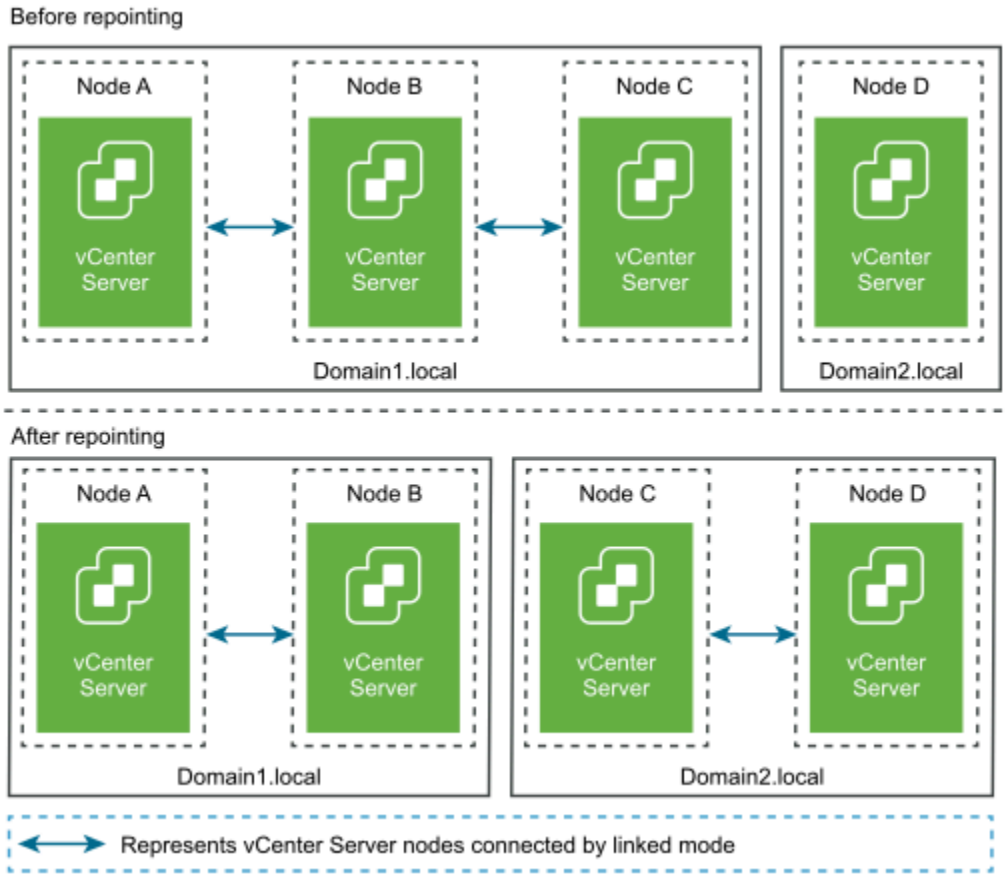
Repoint a vCenter Server Node to an Existing Domain with a Replication Partner

You can repoint a vCenter Server from one Single Sign-On domain to an existing domain using a replication partner.

- Repointing is only supported with vCenter Server 6.7 Update 1 and later.
- You must repoint to a vCenter Server that is of the same version and nodes that are of the same version and build number.
- To ensure no loss of data, take a file-based backup of each node before proceeding with repointing the vCenter Server.

See Figure 25: Repointing a vCenter Server from One Domain to an Existing Domain for an example of repointing to an existing domain. In this case, there is replication.

Figure 25: Repointing a vCenter Server from One Domain to an Existing Domain



1. Shut down the node (for example, Node C) that is being repointed (moved to a different domain).
2. Decommission the vCenter Server node that is being repointed. For example, to decommission Node C, log into Node B (on the original domain) and run the following command:

   ```
   cmsso-util unregister --node-pnid Node_C_FQDN --username Node_B_sso_administrator@sso_domain.com --pass-
   wd Node_B_sso_adminuser_password
   ```

   After unregistering Node C, services are restarted. References to Node C are deleted from Node B and any other nodes that were linked with Node C on the original domain.
3. Power on Node C to begin the repointing process.
4. Optional: Run the pre-check mode command. The pre-check mode fetches the tagging (tags and categories) and authorization (roles and privileges) data from the vCenter Server. Pre-check does not migrate any data, but checks the conflicts between the source and destination vCenter Server. For example, run the pre-check with the following CLI:

   ```
   cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQD-
   N_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name desti-
   nation_PSC_domain
   ```

   Note: Pre-check is not required if a replication partner does not exist (repointing to a newly created domain).

   See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

   The pre-check writes the conflicts to the `/storage/domain-data` directory.

5. Optional: Check conflicts and apply resolutions for all conflicts or apply a separate resolution for each conflict.

   The conflict resolutions are:

   - Copy: Create a duplicate copy of the data in the target domain.
   - Skip: Skips copying the data in the target domain.
   - Merge: Merges the conflict without creating duplicates.

   Note: The default resolution mode for Tags and Authorization conflicts is Copy, unless overridden in the conflict files generated during pre-check.

6. Run the execute command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain. For example, run the execute command with the following:

   ```
   cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN
    _of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-do-
   main-name destination_PSC_domain
   ```

   See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

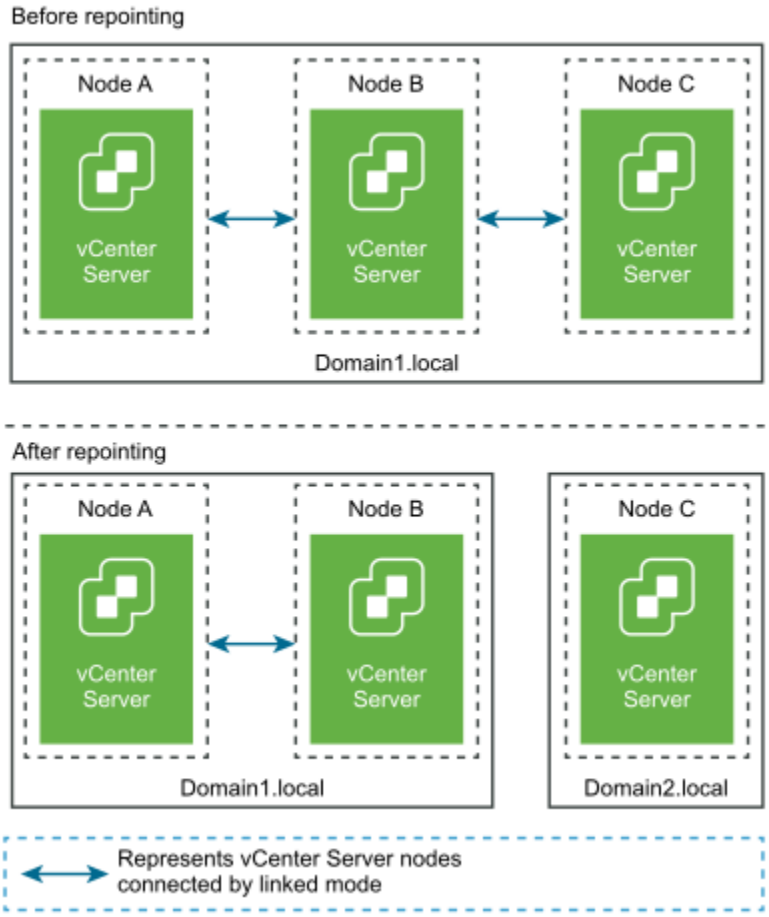
Repoint a vCenter Server Node to a New Domain

You can repoint a vCenter Server from an existing domain to a newly created domain.

- Repointing is only supported with vCenter Server 6.7 Update 1 and later.
- You must repoint to a vCenter Server that is of the same version and nodes that are of the same version and build number.
- To ensure no loss of data, take a file-based backup and a snapshot in powered-off state of each node before proceeding with repointing the vCenter Server.

See Figure 26: Repointing a vCenter Server from One Domain to a New Domain for an example of repointing to a new domain. In this case, there is no replication partner.

Figure 26: Repointing a vCenter Server from One Domain to a New Domain



1. Shut down the node (for example, Node C) that is being repointed (moved to a different domain).

   Note:

   If the vCenter Server is part of a vCenter Server HA cluster, remove the vCenter Server HA configuration before proceeding with the domain repoint. For more information, see *vSphere Availability*.

2. Decommission the vCenter Server node that is being repointed. For example, to decommission Node C, log into Node B (on the original domain) and run the following command:

   ```
   cmsso-util unregister --node-pnid Node_C_FQDN --username Node_B_sso_administrator@sso_domain.com --pass-
   wd Node_B_sso_adminuser_password
   ```

   After unregistering Node C, services are restarted. References to Node C are deleted from Node B and any other nodes that were linked with Node C on the original domain.

3. Power on Node C to begin the repointing process.

4. Run the execute command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain. For example, repointing with no replication partner (repointing to a new domain), run the execute command with the following:

   ```
   cmsso-util domain-repoint -m execute --src-emb-admin Administrator  --dest-domain-name destination_PSC_do-
   main
   ```

   See Syntax of the Domain Repoint Command for argument definitions for the `cmsso-util domain-repoint` command.

Syntax of the Domain Repoint Command

You can use command arguments to set the execution parameters of the domain-repoint command.

The `cmsso-util domain-repoint` CLI repoints vCenter Server from one domain to another.

You can add a space-separated list of arguments to the CLI repoint command

Use the following command to repoint a vCenter Server to another vCenter Server node:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN _of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-domain-name destination_PSC_domain
```

Argument	Description
`-m`, `--mode`	*mode* can be `pre-check` or `execute`. The `pre-check` argument runs the command in pre-check mode. The `execute` argument runs the command in execute mode.
`-spa`, `--src-psc-admin`	SSO administrator user name for the source vCenter Server. Do not append the `@`*domain*.
`-dpf`, `--dest-psc-fqdn`	The FQDN of the vCenter Server to repoint.
`-dpa`, `--dest-psc-admin`	SSO administrator user name for the destination vCenter Server. Do not append `@`*domain*.
`-ddn`, `--dest-domain-name`	SSO domain name of the destination vCenter Server.
`-dpr`, `--dest-psc-rhttps`	(Optional) HTTPS port for the destination vCenter Server. If not set, the default `443` is used.
`-dvf`, `--dest-vc-fqdn`	The FQDN of the vCenter Server pointing to a destination vCenter Server. The vCenter Server is used to check for component data conflicts in the pre-check mode. If not provided, conflict checks are skipped and the default resolution (COPY) is applied for any conflicts found during the import process. **Note:** This argument is optional only if the destination domain does not have a vCenter Server. If a vCenter Server exists in the destination domain, this argument is mandatory.
`-sea`, `--src-emb-admin`	Administrator for the vCenter Server with embedded vCenter Server. Do not append `@domain` to the administrator id.
`-rpf`, `--replication-partner-fqdn`	(Optional) The FQDN of the replication partner node to which the vCenter Server is replicated.
`-rpr`, `--replication-partner-rhttps`	(Optional) The HTTPS port for the replication node. If not set, the default is `443`.
`-rpa`, `--replication-partner-admin`	(Optional) SSO administrator user name of the replication partner vCenter Server.
`-dvr`, `--dest-vc-rhttps`	(Optional) The HTTPS port for the vCenter Server pointing to the destination vCenter Server. If not set, the default `443` is used.
`--ignore-snapshot`	(Optional) Ignore snapshot warnings.
`--no-check-certs`	(Optional) Ignore certification validations.
`--debug`	(Optional) Retrieves command execution detail.
`-h`, `--help`	(Optional) Displays the help message for the `cmsso-util domain repoint` command.

Understanding Tagging and Authorization Conflicts

When you run the domain repoint command in pre-check mode, data from the vCenter Server is exported, examined, and conflicts are written to a file.

The following data is exported to the `/storage/domain-data/` or `ProgramData/VMWare/vCenterServerdata/domain-data` folder:

- `All_Privileges.json`
- `All_Roles.json`
- `All_TagCategories.json`
- `All_Tags.json`

These files contain the all the data (Authorization and Tagging) from the vCenter Server on which this command was run.

If a secondary vCenter Server is provided using the `-dvf` or `--dest-vc-fqdn` option, any conflicts are also exported to the same folder:

- `Conflicts_Roles.json`
- `Conflicts_TagCategories.json`
- `Conflicts_Tags.json`

The following is a sample conflicts file:

```
<---- Sample Conflict file code block --->
  {
  "global" : {
    "resolution" : "MERGE|SKIP|COPY",
    "description" : "Default resolution option used to resolve Role Conflicts is COPY. The
conflicts list describes the differences between Role entities on source and target vCenter Server. If
the source information represents an empty JSON array, it simply means that all the entity
attributes from source and target are identical. If the source lists few entries, it means
that only these entity attributes are missing from the target. If the target lists few entries,
it means that only these entity attributes are missing from the source. Though a global resolution
can be set, it can also be overridden at each conflict level by providing individual resolution
mode."
  },
  "conflicts-count" : 1,
  "conflicts-list" : {
    "NoCryptoAdmin" : {
      "source" : {
        "privileges" : "[]"
      },
      "target" : {
        "privileges" : "[Group-1.SamplePriv-1, Group-1.SamplePriv-4, Group-2.SamplePriv-10,
Group-2.SamplePriv-3, Group-2.SamplePriv-7, Group-3.SamplePriv-2, Group-3.SamplePriv-9]"
      },
      "resolution" : ""
    }
}
<----- End of code block --->
```

The parts of the sample conflict files are:

- `description` . Provides the details on how the respective conflicts file is read and understood.

- `source` and `target` . JSON objects that list only the differences between the source and target vCenter Server objects.
- `resolution` . User supplies one valid resolution. Valid resolutions are `MERGE` , `COPY` , and `SKIP` .

To specify the resolution for handling conflicts, you can provide a default resolution option all conflicts in the `"global": "resolution" = "MERGE|SKIP|COPY"` section. If you do not provide a valid global resolution type for `resolution` or leave it unedited, the system uses `COPY` as the default resolution option.

You can also provide a valid resolution option for each of the conflicts by editing the `resolution` property at each conflict level which overrides the global resolution option.

The types of conflicts listed in Table 56: Conflict Types.

Table 56: Conflict Types

Conflict	Properties used to compare Category Objects	Conflict Types	Conflicting Properties	Conflict Resolution Options
Role conflict	• `name` : Name of the category. • `privilegeId` : List of privileges for the role.	`RoleName` conflict occurs while importing roles and a role with the same name exists in the target vCenter Server but with different privileges.	Properties that can be conflicting for `RoleName` conflict type can be `Privileges` .	• `COPY` . A copy of the conflicting role is created in the target vCenter Server, with `--copy` appended to the role name. The new role is created with a new role ID with the same set of privilege IDs. The new role ID is updated in the `VPX_ACCESS` table. The new role ID is applicable for both role name conflict and role ID conflict. **Note:** The default resolution option to resolve Role conflicts is `COPY` . • `MERGE` .The `MERGE` option is resolved in the following sequence: a. If the source vCenter Server has a role with the same name and privilege list as a role in the target vCenter Server, but the role IDs are different, the role ID from the target vCenter Server is used and updated in the `VPX_ACCESS` table. b. If the source vCenter Server has a role with the same name as a role in the target vCenter Server, but with a different privilege list, then the privilege lists for both roles are merged. • `SKIP` . Do nothing. The specific role is skipped.

Conflict	Properties used to compare Category Objects	Conflict Types	Conflicting Properties	Conflict Resolution Options
Tag Category conflict: A category name must be unique in a vCenter Server.	• `name` : Name of the category. • `cardinality` : Cardinality of Category, either Single or Multiple. • `associableEntityType` : List of vCenter Server object that can be associated with a tag from this category. A value of `All` indicates all vCenter Server objects.	Only one type of conflict can be seen while importing Tag Categories, `CategoryName` conflict. This conflict indicates that a category with the same name exists in the target vCenter Server but with different properties (`cardinality` or `associableEntityType`).	Properties that can be conflicting for conflict type `CategoryName` can be at least one of two types: `Cardinality` or `AssociableTypes` .	• `COPY` . A copy of the conflicting category is created in the target vCenter Server, with `--copy` appended to the category name. The new category is created with the same property name as in the source vCenter Server. All the tags that were present under this category is imported under the newly created `CategoryCopy` . **Note:** The default resolution option to resolve `CategoryName` conflicts is `COPY` . • `MERGE` . Conflicting properties are merged with the category that is already present in the SSO. Properties are merged as follows: 1. `Description` . The description that is already present is used. 2. `Cardinality` . Cardinality cannot shrink. If there is a cardinality conflict, the cardinality is set to `multiple` . It cannot be reduced to single. 3. `AssociableTypes` .If either the `associableEntityType` values are null, it is set to null. Otherwise, `Objects` types are merged. • `SKIP` . Do nothing. All tags are imported under the category that exists.
Tags Conflict: A `tag` object always belongs to a `category` Object. A tag Name must be unique only inside a category.	• `name` • `description`	Only one type of conflict can be seen while importing tags: `TagName` conflict. This conflict indicates that a Tag with the same name exists under the same category and in the target vCenter Server but with different properties.	Properties that can be conflicting for a conflict of type: `TagName` can be `Description` .	• `COPY` . A copy of the conflicting tag is created in the target vCenter Server, with `--copy` appended to the tag name. Take the `MoRef` (Internal tag ID) of the newly created tag and update the tag association if necessary. **Note:** The default resolution option to resolve `CategoryName` conflicts is `COPY` .

Conflict	Properties used to compare Category Objects	Conflict Types	Conflicting Properties	Conflict Resolution Options
				• `MERGE` .Keep the existing description. Take the `MoRef` (Internal Tag ID) and update one or more Tag Associations if necessary. • `SKIP` . Do nothing. Do not create this tag. Clean up any Tag Associations.

vCenter Server Domain Repoint License Considerations

Domain repointing copies license keys to a new domain. Copying the license keys ensures that valid licensing of all assets is maintained after repointing.

vCenter Server tracks license usage on a per domain basis. If a key is used in more than one domain, you must ensure that the aggregate use of the key does not exceed its capacity. To simplify your license management, remove each license copied to a second domain and assign a new license to assets.

Consider the following two cases:

- License keys that are no longer in use (that is, assigned to assets) in the original domain post repointing.
- License keys that are in use (that is, assigned to assets) in multiple domains.

License Keys Not in Use in a Domain

License Keys in Use in Multiple Domains

If after completing repointing, a license key is in use (that is, assigned to assets) in more than one domain, to remove the license key from all but one domain, first a different license key must be assigned to each asset in domains from which the license key will be removed. Two common approaches:

Troubleshooting vCenter Server Installation or Deployment

The vCenter Server deployment troubleshooting topics provide solutions to problems that you might encounter during the vCenter Server appliance deployment process.

Collecting Logs for Troubleshooting a vCenter Server Installation or Upgrade

You can collect installation or upgrade log files for vCenter Server. If an installation or upgrade fails, checking the log files can help you identify the source of the failure.

You can also collect deployment log files for vCenter Server.

Retrieve Installation Logs Manually

You can retrieve the installation log files manually for examination.

1. Navigate to the installation log file locations.
   - `%PROGRAMDATA%\VMware\vCenterServer\logs` directory, usually `C:\ProgramData\VMware\vCenterServer\logs`
   - `%TEMP%` directory, usually `C:\Users\`*`username`*`\AppData\Local\Temp`

The files in the `%TEMP%` directory include `vc-install.txt`, `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log`, and `vim-vcs-msi.log`.

Note:

- In Linux, the installation logs are in `/tmp/vcsaUiInstaller`
- In MacOS, the installation logs are in `/var/folders/**/vcsaUiInstaller`
  The installer randomly picks a temporary folder to place the log files. Locate the `vcsaUiInstaller` folder within `/var/folders/` for the log files.

2. Open the installation log files in a text editor for examination.

Related Links

Collect Deployment Log Files for the vCenter Server Appliance on page 1298
If the vCenter Server appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

Export a vCenter Server Support Bundle for Troubleshooting on page 1298
You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

Collect Deployment Log Files for the vCenter Server Appliance

If the vCenter Server appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

The full path to the log files is displayed in the vCenter Server appliance deployment wizard.

In case of firstboot failure, you can download the support bundle on a Windows host machine and examine the log files to determine which firstboot script failed. See Export a vCenter Server Support Bundle for Troubleshooting.

1. On the Windows machine that you use for deploying the vCenter Server appliance, navigate to the log files folder.
   If you are logged in as an administrator, by default this is the `C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller` folder.
2. Open the installation log files in a text editor for examination.

Related Links

Retrieve Installation Logs Manually on page 1297
You can retrieve the installation log files manually for examination.

Export a vCenter Server Support Bundle for Troubleshooting on page 1298
You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

Export a vCenter Server Support Bundle for Troubleshooting

You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

You can also collect the support bundle from the vCenter Server appliance Bash shell by running the `vc-support.sh` script.

The support bundle is exported in `.tgz` format.

1. Log in to the Windows host machine on which you want to download the bundle.
2. Open a Web browser and enter the URL to the support bundle displayed in the DCUI.
   https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle

3. Enter the user name and password of the root user.
4. Click **Enter**.

   The support bundle is downloaded as `.tgz` file on your Windows machine.

Related Links

Retrieve Installation Logs Manually on page 1297
You can retrieve the installation log files manually for examination.

Collect Deployment Log Files for the vCenter Server Appliance on page 1298
If the vCenter Server appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

vCenter Server Upgrade

vCenter Server Upgrade describes how to upgrade VMware vCenter Server™ to the current version.

To move to the current version of vCenter Server by performing a fresh installation that does not preserve the existing configuration of your environment, see the vCenter Server Installation and Setup documentation.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

vCenter Server Upgrade is for anyone who must upgrade from earlier versions of vSphere. These topics are for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

vCenter Server Upgrade Options

vCenter Server7.0 provides many options for upgrading your vCenter Server deployment. For a successful vCenter Server upgrade, you must understand the upgrade options, the configuration details that impact the upgrade process, and the sequence of tasks.

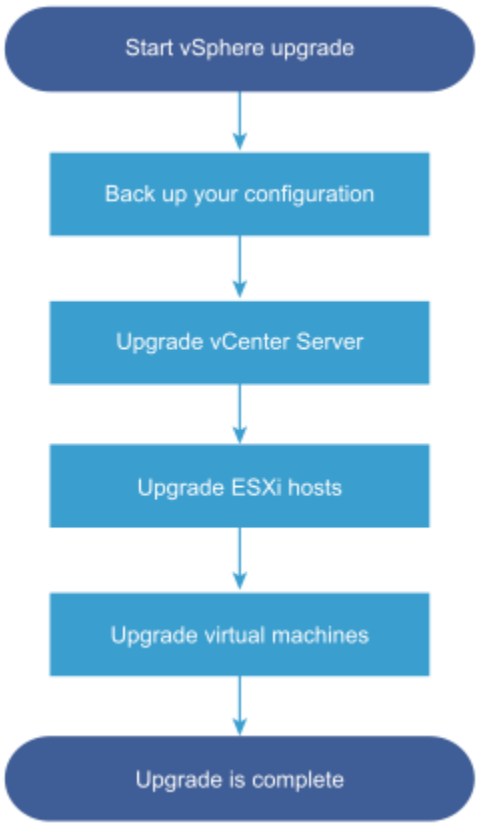
The two core components of vSphere are VMware ESXi™ and VMware vCenter Server™. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. You use the vCenter Server system to pool and manage the resources of multiple hosts. vCenter Server appliance is a preconfigured virtual machine optimized to run vCenter Server.

You can upgrade existing vCenter Server deployments that include either an embedded or an external Platform Services Controller to a deployment consisting of a vCenter Server appliance.

Overview of the vSphere Upgrade Process

vSphere is a sophisticated product with multiple components to upgrade. Understanding the required sequence of tasks is vital for a successful vSphere upgrade.

Figure 27: Overview of vSphere Upgrade Tasks



Upgrading vSphere includes the following tasks:

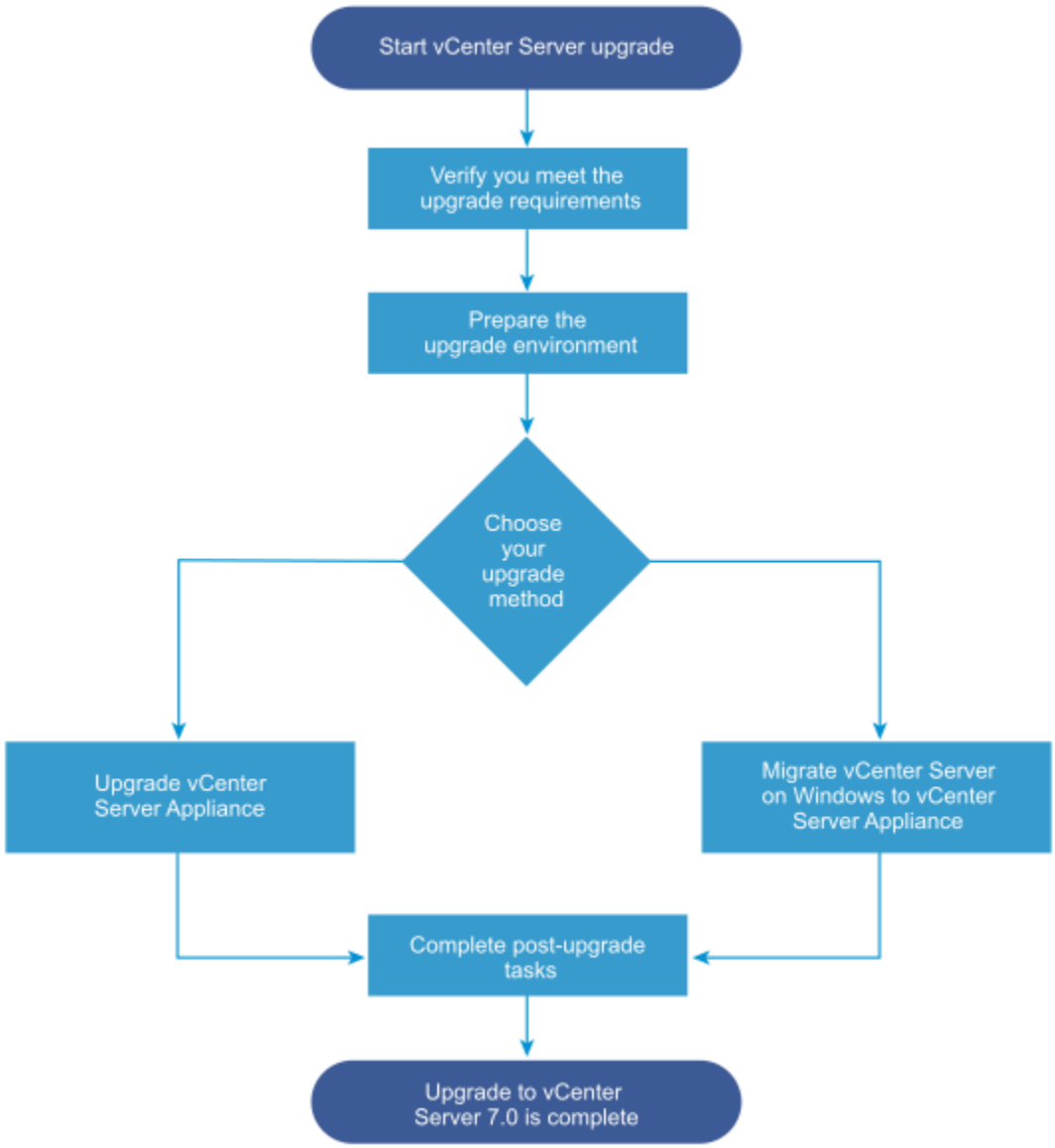
1. Read the vSphere release notes.
2. Verify that you have backed up your configuration.
3. If your vSphere system includes VMware solutions or plug-ins, verify that they are compatible with the vCenter Server appliance version to which you are upgrading. See *VMware Product Interoperability Matrix* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
4. Upgrade vCenter Server.
5. To ensure sufficient disk storage for log files, consider setting up a syslog server for remote logging. Setting up logging on a remote host is especially important for hosts with a limited amount of local storage.
6. Upgrade your VMs manually or by using vSphere Lifecycle Manager to perform an orchestrated upgrade.

Overview of the vCenter Server Upgrade Process

VMware provides many options to upgrade to vCenter Server7.0.

You can upgrade or migrate your vCenter Server version 6.5 or version 6.7 installation to version 7.0 .

Figure 28: Overview of vCenter Server Upgrade Tasks



High-level steps for upgrading or migrating vCenter Server:

1. Select your upgrade goal.
   - Upgrading the vCenter Server Appliance
   - Migrating vCenter Server for Windows to Appliance
2. Verify that your system meets the hardware and software requirements.
3. Prepare your environment for the upgrade or migration.
4. Upgrade or migrate your vCenter Server for Windows or vCenter Server appliance deployment.
5. Finish any required post-upgrade or post-migration tasks.

Concurrent upgrades are not supported and upgrade order matters. For information on the order in which to upgrade transitional environments, see Example Upgrade Paths from vCenter Server 6.5 and 6.7 to vCenter Server7.0.

vCenter Server Supported Upgrade Methods

Graphical User Interface (GUI) Installer	The GUI installer provides a two-step upgrade method using an OVA file that you deploy, and the vCenter Server appliance Management GUI. The first step deploys vCenter Server appliance as an OVA file. The second step uses the vCenter Server Management GUI to configure the new appliance using the source deployment data.
Command Line Interface (CLI) Installer	The CLI installer provides advanced users with a CLI method for upgrading the vCenter Server appliance or migrating vCenter Server for Windows to an appliance. You can upgrade or migrate to a vCenter Server appliance using customized CLI templates.
Migration Assistant Interface for Migrating vCenter Server for Windows to vCenter Server appliance	When you migrate a legacy Platform Services Controller or vCenter Server for Windows to an appliance using the Migration Assistant interface. You can use either the GUI method or the CLI method to migrate the legacy Windows installation data to a target appliance. See Overview of Migration from vCenter Server on Windows to vCenter Server Appliance.
Deprecated vCenter Server Deployment Models	When upgrading or migrating from deprecated deployment models, you must first migrate your deployment to a currently supported deployment model before attempting to upgrade or migrate it to a vCenter Server7.0 deployment. For more information, see Moving from a Deprecated to a Supported vCenter Server Deployment Topology Before Upgrade or Migration
Patching and Updating vCenter Server	A patch or update brings the vCenter Server7.0 software up to the current, minor version. You can use the patching process to make minor upgrades to your 7.0 deployment. See Differences Between vSphere Upgrades, Patches, Updates, and Migrations and Patching and Updating vCenter Server7.0 Deployments.

vCenter Server Upgrade Compatibility

The upgrade to vCenter Server7.0 affects other software components of the data center.

Table 57: Upgrading vCenter Server and Related VMware Products and Components summarizes how upgrading vCenter Server can affect your data center components.

vCenter Server7.0 can manage ESXi version 6.5 hosts in the same cluster with ESXi7.0 hosts. vCenter Server7.0 cannot manage ESXi 6.0 or earlier hosts.

vSphere supports upgrades from vCenter Server 6.5 and later to vCenter Server 7.0. To upgrade from vCenter Server 5.0, 5.1, 5.5, or 6.0 you must first upgrade the vCenter Server instance to version 6.5 or later releases, and then upgrade to vCenter Server 7.0. For information about upgrading vCenter Server 5.0, 5.1, 5.5, or 6.0 to version 6.5 or 6.7, see the *VMware vSphere 6.5 Documentation* or *VMware vSphere 6.7 Documentation*

Table 57: Upgrading vCenter Server and Related VMware Products and Components

Product or Component	Compatibility
vCenter Server	Verify support for the upgrade path from your current version of vCenter Server to your planned upgrade version. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Product or Component	Compatibility
vCenter Server database	Verify that your database is supported for the vCenter Server version that you are upgrading to. Upgrade the database if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. **Note:** vCenter Server7.0 uses PostgreSQL for the embedded database. vCenter Server 7.0 does not support external databases.
ESX and ESXi hosts	Verify that your ESX or ESXi host works with the vCenter Server version that you are upgrading to. vCenter Server7.0 requires ESXi host version 6.5 or later. Upgrade if necessary. See the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
VMware Host Profiles	Host Profiles is a vCenter Server tool for designing and deploying ESX and ESXi hosts. Ensure that you are using Host Profiles version 6.0 or later. See Knowledge Base article KB 52932. For more information on upgrade problems related to Host Profiles, see Upgrade Issues with vCenter Server Containing Host Profiles and the sections on Host Profiles upgrade workflows in the *vSphere Host Profiles* documentation.
VMFS volumes	ESXi no longer supports VMFS3 datastores. The ESXi host automatically upgrades VMFS3 to VMFS5 when mounting existing datastores. You cannot upgrade a VMFS5 datastore to VMFS6. If you have a VMFS5 datastore in your environment, create a VMFS6 datastore and migrate virtual machines from the VMFS5 datastore to VMFS6. For more information on VMFS datastores, see the *vSphere Storage* documentation.
Virtual machines	Upgrade options depend on your current version. See the information about upgrading virtual machines in the *ESXi Upgrade* documentation.
VMware Tools	Upgrade options depend on your current version. See the information about upgrading VMware Tools in the *ESXi Upgrade* documentation.
Auto Deploy	To ensure compatibility and best performance, when you upgrade to vCenter Server7.0, use Auto Deploy to upgrade ESXi hosts to the same version.
vSphere Distributed Virtual Switch (DVS)	You must upgrade to DVS version 6.5 or later before you upgrade to vCenter Server7.0. See Knowledge Base article KB 52826.
vSphere Network I/O Control	DVS version 6.0 or later supports only Network I/O Control version 3. If you are using an earlier version of Network I/O Control you must upgrade to Network I/O Control version 3. For more information, see the *vSphere Networking* documentation.
vSAN	To avoid potential faults because of differences in the vSAN support in vCenter Server and ESXi, synchronize versions of vCenter Server and ESXi. For the best integration between vSAN components on vCenter Server and ESXi, deploy the latest version of these two vSphere components. For more information, see the *ESXi Installation and Setup*, *vCenter Server Installation and Setup*, *ESXi Upgrade*, and *vCenter Server Upgrade* documentation.
vSAN disk version	vSAN has several different on-disk format versions available depending on the version and upgrade history of the cluster. Some on-disk format versions are transient while others are intended for long-term production. As certain vSAN features are tied to the on-disk format version, the format version must be accounted for when determining interoperability. See Knowledge Base article KB 2148493.
Legacy Fault Tolerance	If the vCenter Server inventory contains a VM on which legacy VMware Fault Tolerance (FT) is in use, upgrade or migration will be blocked until you turn off this feature. For information about legacy FT, see Knowledge Base article KB 2143127. For information on disabling or turning off FT, see Knowledge Base article KB 1008026.

vCenter Server7.0 Component Behavior Changes That Affect Upgrade

When upgrading to vCenter Server7.0, it is important to understand changes in component behavior for version 7.0 that can affect the upgrade process.

Understanding changes from previous versions of vSphere can help in your upgrade planning. For a complete list of new features in vSphere 7.0, see the Release Notes for version 7.0 releases.

vCenter Server Upgrade Methods

There are multiple methods for upgrading vCenter Server to version 7.0.

Supported Migration Path from vCenter Server for Windows to vCenter Server	You can migrate from an existing vCenter Server for Windows to a vCenter Server7.0 deployment using a graphical user interface-based installer or a command-line interface-based installer. See Migrating vCenter Server for Windows to Appliance .
Support for Graphical User Interface (GUI) Deployments of vCenter Server	You can upgrade an existing vCenter Server appliance version 6.5 or 6.7 deployment to vCenter Server7.0 using the GUI. See GUI Upgrade of the vCenter Server Appliance.
Support for Command Line Interface (CLI) Deployments of vCenter Server Appliance	You can upgrade an existing vCenter Server appliance version 6.5 or 6.7 deployment to vCenter Server7.0 using the CLI. See CLI Upgrade of the vCenter Server Appliance .
VMware Update Manager Changes	You can use a graphical user interface (GUI) when upgrading vCenter Server deployments using VMware Update Manager.

Changes in Supported Deployment Types

Changes from previous versions of vSphere can affect your deployment type.

Mixed IPv4 and IPv6 Upgrade and Migration

- Upgrade and migration from vCenter Server 6.5 or 6.7 to 7.0 is supported for pure IPv4 or pure IPv6 management networks only.
- Using dual IP stacks (IPv4 and IPv6) is not supported.

Removal of Platform Services Controller

Beginning in vSphere 7.0, deploying or upgrading vCenter Server in vSphere 7.0 requires the use of vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server.

The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management.

Upgrade or Migration for vCenter Server Instances with an External Platform Services Controller

When you upgrade or migrate a vCenter Server deployment using an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the upgrade or migration.

When you converge the Platform Services Controller into a vCenter Server appliance, you must identify the management node to use for your deployment's vSphere SSO domain. In domains with multiple vCenter Server instances, you must specify the SSO replication partner to use for each subsequent vCenter Server.

The method you use to upgrade or migrate determines how you specify the management node to use for your deployment's vSphere SSO domain.

- If you upgrade or migrate using the GUI-based installer, the Upgrade wizard prompts you to specify the replication topology for the vCenter Server deployment.
  To learn about upgrading using the GUI-based installer, see Upgrade a vCenter Server Appliance 6.5 or 6.7 with an External Platform Services Controller Instance by Using the GUI. To learn about migrating using the GUI-based installer, see GUI Migration of vCenter Server with an External Platform Services Controller to an Appliance.
- If you upgrade or migrate using the CLI-based installer, you specify the replication topology for the vCenter Server deployment using the JSON templates. The JSON files contain the configuration parameters and their values for your upgrade or migration specification.
  To learn about upgrading using the CLI-based installer, see About Upgrading a vCenter Server with an External Platform Services Controller Using the CLI. To learn about migrating using the CLI-based installer, see About Migrating a vCenter Server for Windows with an External Platform Services Controller Using the CLI.

When the upgrade or migration process finishes, the newly deployed vCenter Server7.0 appliance incorporates the former Platform Services Controller services. You can then decommission the external Platform Services Controller in your environment. See Decommission the Platform Services Controller.

To learn more about converging a vCenter Server deployment using an external Platform Services Controller into a vCenter Server appliance, see Knowledge Base article KB 68137.

Upgrading or Migrating to vSphere License Service

The License Service provides common license inventory and management capabilities to the systems. When upgrading or migrating your deployment, licensing data is transferred to the License Service in the vCenter Server appliance.

When upgrading versions 6.5 or 6.7 that are connected to a Platform Services Controller, their licensing data is transferred to the License Service in the vCenter Server appliance. The licensing data includes the available licenses and license assignments for hosts, systems, vSAN clusters, and other products that you use with vSphere.

After the upgrade or migration of the systems finishes, the License Services stores the available licenses and manages the license assignments for the entire vSphere environment.

For more information about the License Service and managing licenses in vSphere, see *vCenter Server and Host Management*.

Upgrading the Trust Authority vCenter Server

Upgrade the Trust Authority vCenter Server and Trust Authority Hosts.

Starting with vSphere 7.0, you can take advantage of VMware® vSphere Trust Authority™. vSphere Trust Authority is a foundational technology that enhances workload security. vSphere Trust Authority establishes a greater level of trust in your organization by associating an ESXi host's hardware root of trust to the workload itself.

The best practice for upgrading a vSphere Trust Authority infrastructure is to upgrade the Trust Authority vCenter Server and Trust Authority Hosts first. In this way, you get the most benefit from the latest vSphere Trust Authority features. However, you can perform separate, standalone upgrades of vCenter Server and ESXi hosts to fit specific business reasons. To learn about upgrading the Trust Authority Cluster vCenter Server see "vSphere Trust Authority Life Cycle" in the *vSphere Security* guide.

Differences Between vSphere Upgrades, Patches, Updates, and Migrations

vSphere products distinguish between upgrades, which make major changes to the software, patches and updates, which make smaller changes to the software, and migrations, which make changes to the software platform.

VMware product versions are numbered with two digits, for example, vSphere 7.0. A release that changes either digit, for example, from 6.5 to 6.7, or from 6.7 to 7.0, involves major changes in the software, and requires an upgrade from

the previous version. A release that makes a smaller change, requiring only a patch or update, is indicated by an update number, for example, vSphere 6.7 Update 1.

For information about upgrading vCenter Server installations, see Upgrading the vCenter Server Appliance.

For information about patching or updating vCenter Server, see Patching and Updating vCenter Server7.0 Deployments

When you upgrade an ESXi host, some host configuration information is preserved in the upgraded version, and the upgraded host, after rebooting, can join a vCenter Server instance that has been upgraded to the same level. Because updates and patches do not involve major changes to the software, host configuration is not affected. For more information, see the *ESXi Upgrade* documentation.

When you upgrade a vCenter Server for Windows instance and convert it to a vCenter Server appliance instance, it is a migration.

For information about migrating a vCenter Server installation to a, see Migrating vCenter Server for Windows to Appliance .

Support for Upgrading a vCenter Server with Multi-Homing

When upgrading a vCenter Server appliance with two or more network interface cards (NICs), the upgrade transfers the IP addresses from each network interface from the source vCenter Server to the target vCenter Server.

During the upgrade process, the Upgrade installer performs a pre-check of the source vCenter Server and records the network settings. When this information is transferred to the target vCenter Server appliance, the network settings are transferred as part of the configuration. When the upgrade process finishes, you can log in to the vCenter Server appliance using the vSphere Client vSphere Client, and verify that the IP addresses have been successfully transferred to the newly upgraded vCenter Server appliance.

With two or more NICs per vCenter Server appliance, you can better manage network traffic in your environment. For example, with multiple network interfaces you can:

- Configure backup traffic to use a different network than management traffic.
- Keep ESXi hosts on a physically different LAN segment from your management traffic. You can connect one network interface to the network with your ESXi hosts, and connect the other to a network from which administrative clients connect to vCenter Server.

Support for Federal Information Processing Standard 140-2

vCenter Server7.0 supports Federal Information Processing Standard (FIPS) 140-2.

FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. By default, FIPS 140-2 is always enabled after installation or upgrade of vCenter Server7.0.

To learn more about support for FIPS 140-2 in VMware products, see https://www.vmware.com/security/certifications/fips.html.

To learn how to enable or disable FIPS 140-2 support, see the *vSphere Security* documentation.

Support for Transport Security Layer 1.2

By default, vSphere supports the Transport Security Layer (TLS) 1.2 encryption protocol. The upgrade or migration from earlier releases disables the TLS 1.0 and TLS 1.1 encryption protocols, and you might need to reconfigure other VMware products and third-party products to use TLS 1.2.

During both upgrade and migration from, a notification message informs you that only the TLS 1.2 protocol is enabled. If you must use the TLS 1.0 and TLS 1.1 protocols to support products or services that do not support TLS 1.2, use the TLS

Configurator Utility to enable or disable different TLS protocol versions. You can disable TLS 1.0, or you can disable both TLS 1.0 and TLS 1.1.

For a list of VMware products that support disabling TLS 1.0 and TLS 1.1, see VMware Knowledge Base article 2145796. To learn how to manage TLS protocol configuration and use the TLS Configurator Utility, see the *VMware Security* documentation.

Moving from a Deprecated to a Supported vCenter Server Deployment Topology Before Upgrade or Migration

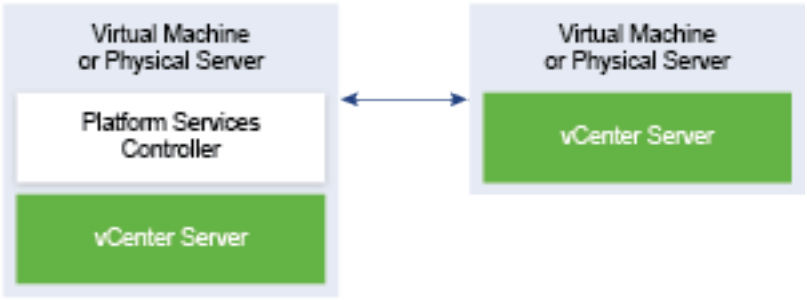
Before you upgrade or migrate your environment to vSphere 7.0, you must move any deprecated deployment topology to a supported deployment topology.

When you first install vCenter Server 6.5 or 6.7, your deployment includes either an embedded Platform Services Controller or an external Platform Services Controller.

The installer does not validate whether the Platform Services Controller is external or embedded with vCenter Server. Although many types of join operations are possible, not all resulting topologies are supported. Before you upgrade or migrate your environment to vSphere 7.0, you must move any deprecated deployment topology to a supported deployment topology.

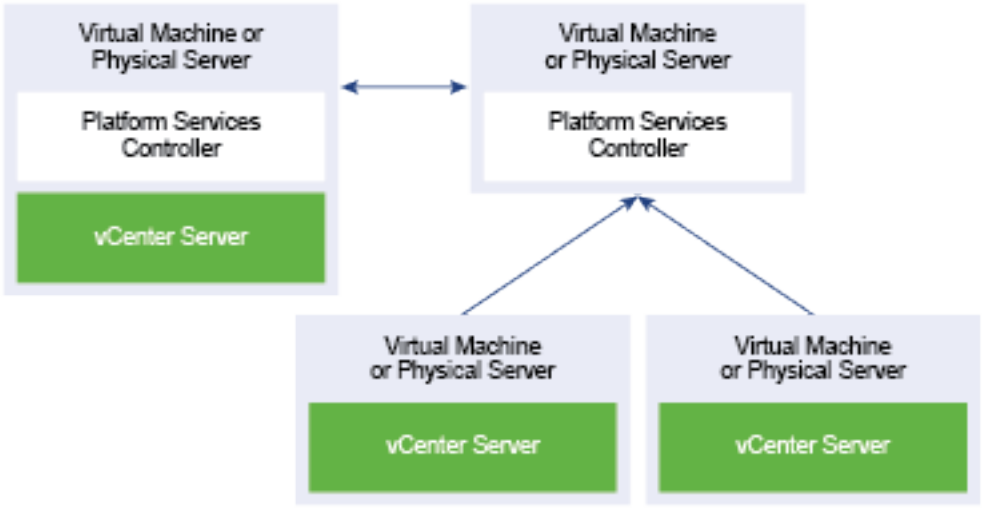
Moving to a Supported Topology from a vCenter Server Pointing to an Embedded Platform Services Controller

Figure 29: Deprecated topology of a vCenter Server Pointing to an Embedded Platform Services Controller



Moving to a Supported Topology from an Embedded Platform Services Controller and an External Platform Services Controller in Replication

Figure 30: Deprecated Topology of an Embedded Platform Services Controller and an External Platform Services Controller in Replication



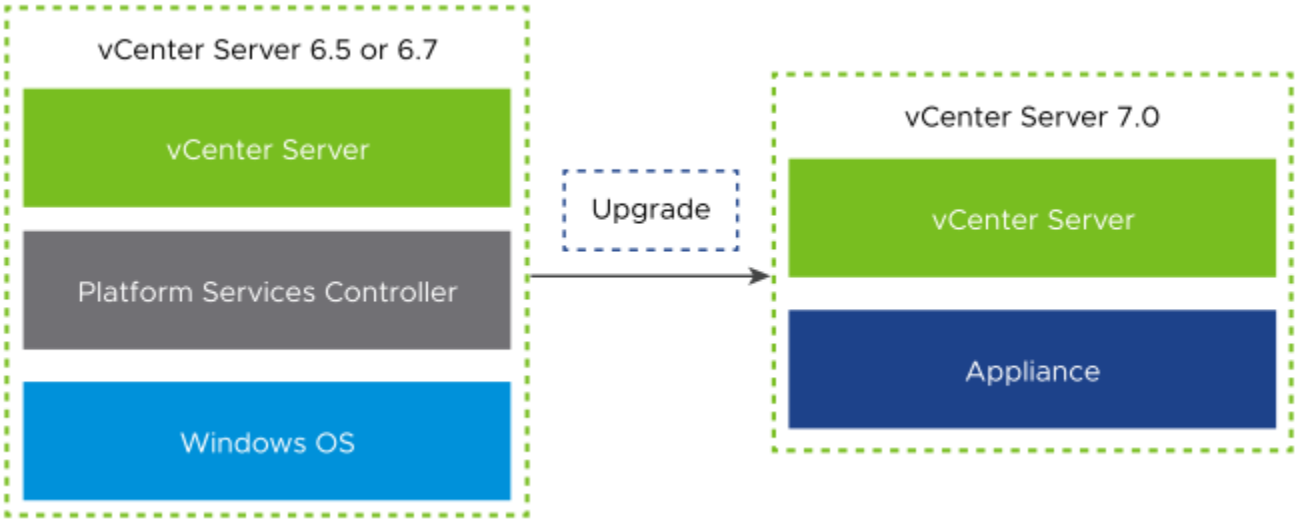
Example Upgrade Paths from vCenter Server 6.5 and 6.7 to vCenter Server7.0

vCenter Server 6.5 and 6.7 deployments upgrade to 7.0.

The vCenter Server example upgrade paths demonstrate vCenter Server 6.5 or 6.7 upgrade outcomes.

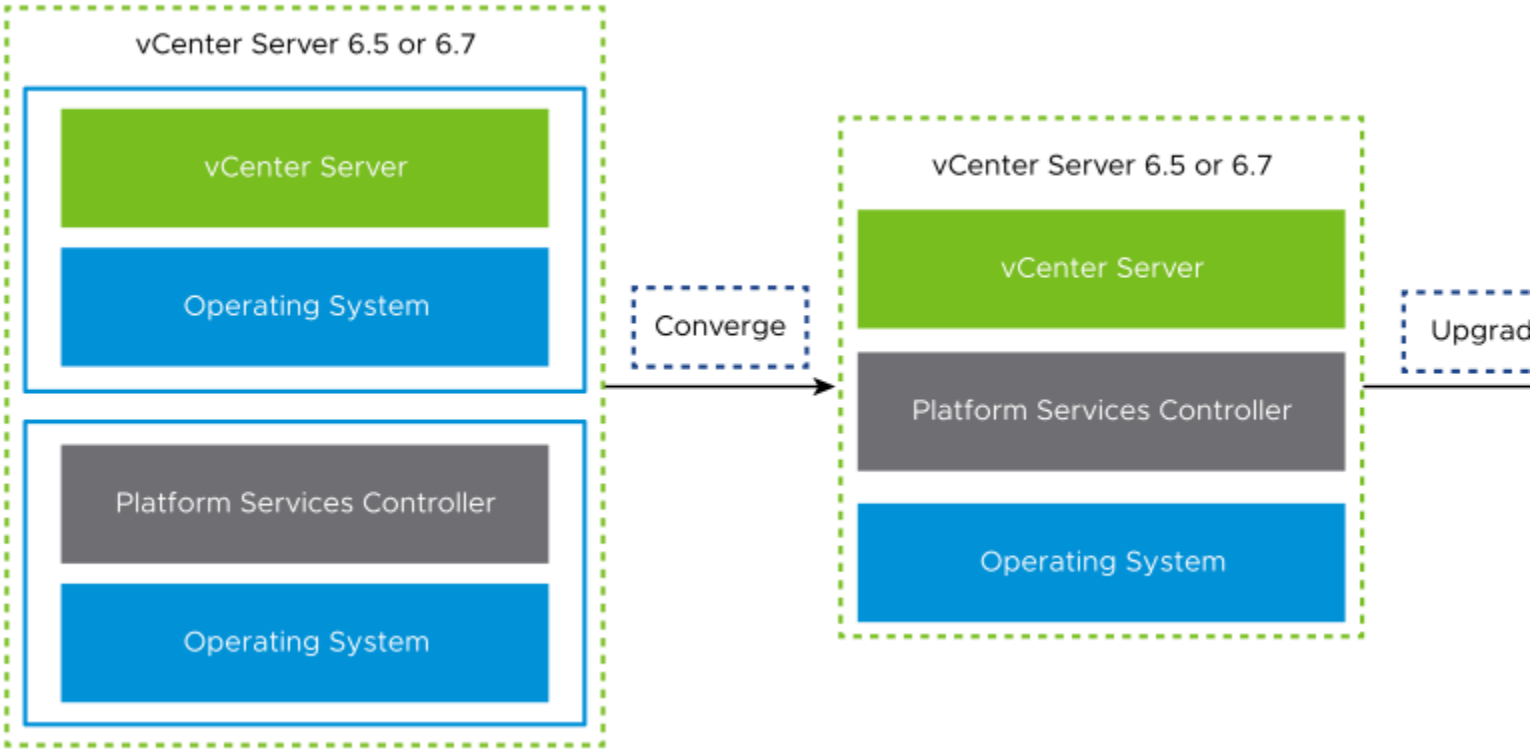
The installer upgrades vCenter Server 6.5 and 6.7 with an embedded Platform Services Controller instance to vCenter Server7.0.

Figure 31: vCenter Server 6.5 or 6.7 with Embedded Platform Services Controller Before and After Upgrade



Before upgrading a vCenter Server deployment with an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the upgrade.

Figure 32: vCenter Server 6.5 or 6.7 with External Platform Services Controller Before and After Upgrade



Example Migration Paths from vCenter Server for Windows to vCenter Server 7.0

You can migrate a vCenter Server for Windows instance to a vCenter Server7.0 instance.

You can migrate a vCenter Server for Windows version 6.5 or 6.7 to a vCenter Server7.0 appliance.

The vCenter Server example migration paths demonstrate supported migration outcomes.

You can migrate a vCenter Server 6.5 or 6.7 instance with an embedded Platform Services Controller to a 7.0. In this case the software migrates the vCenter Server instance and the embedded Platform Services Controller instance at the same time.

Figure 33: vCenter Server 6.5 or 6.7 with Embedded Platform Services Controller Installation Before and After Migration

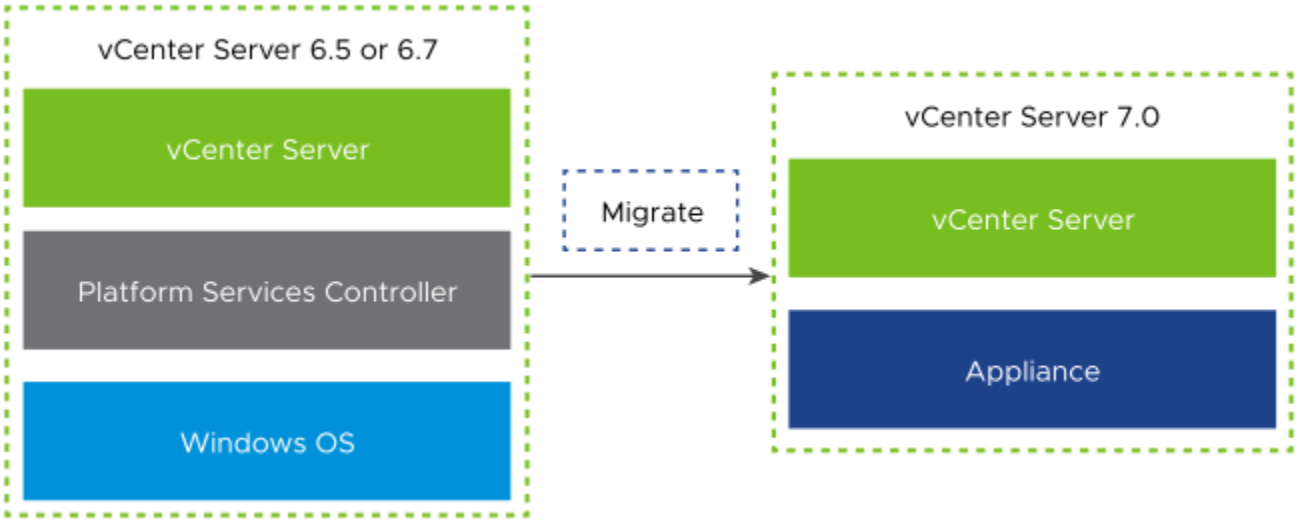
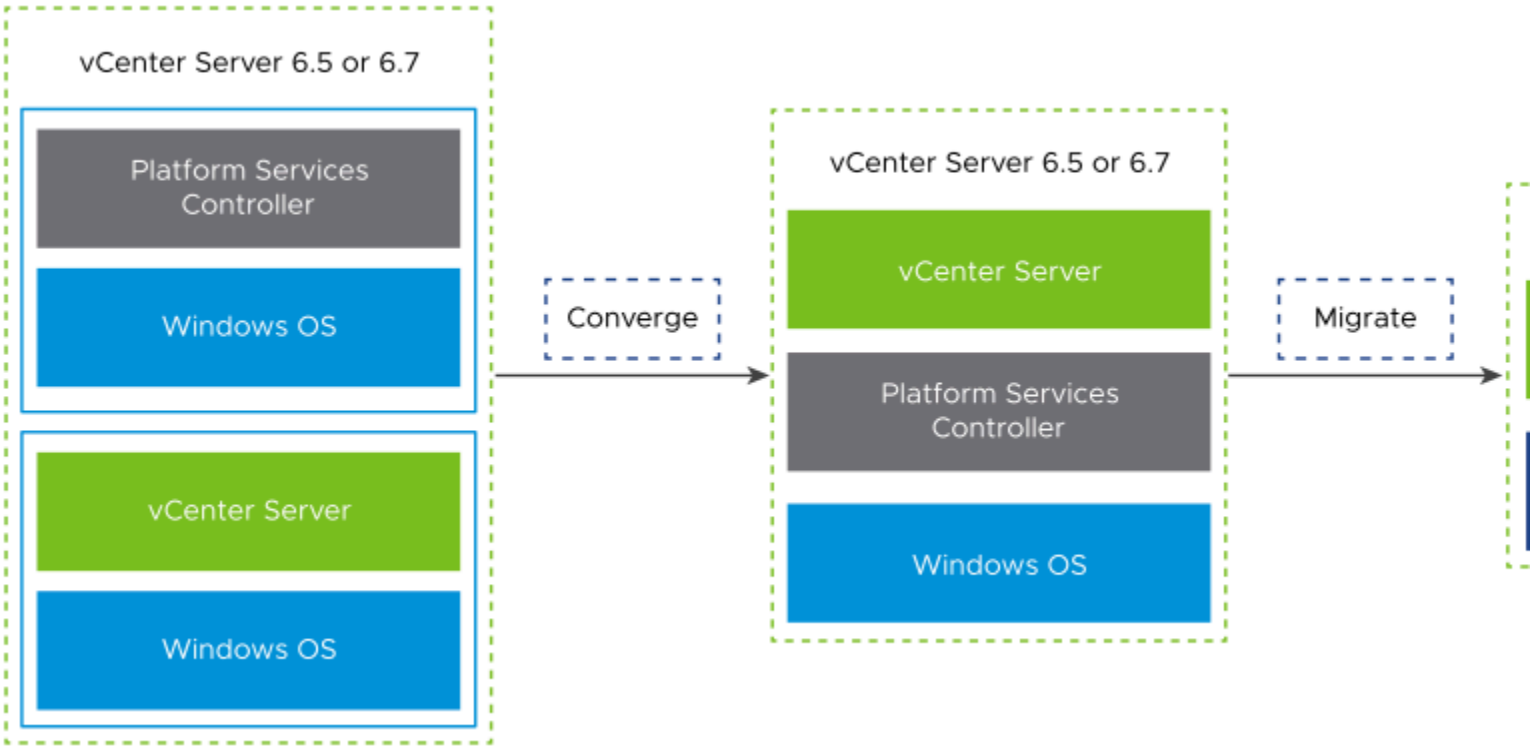


Figure 34: vCenter Server 6.5 or 6.7 with External Platform Services Controller Installation Before and After Migration



Before migrating a vCenter Server 6.5 or 6.7 instance with an external Platform Services Controller, you must converge the external Platform Services Controller to an embedded Platform Services Controller and then migrate to vCenter Server7.0.

Upgrading the vCenter Server Appliance

You can upgrade appliance 6.5 or 6.7 to version 7.0. All the installation files that are necessary for the upgrade are included in the installer, which you can download from the VMware website.

The upgrade of the appliance is a migration of the old version to the new version, which includes deploying a new appliance of version 7.0. You can deploy the new appliance on an ESXi host 6.5 or later, or on the inventory of a instance 6.5 or later. You assign a temporary IP address to the new appliance to facilitate the configuration and services data migration from the old appliance to the newly deployed appliance. After the migration, the IP address and host name of the old appliance are applied to the new upgraded appliance of version 7.0. At the end of the upgrade, the temporary IP address is released and the old appliance is powered off.

Version 7.0 of uses an embedded PostgreSQL database. During the upgrade, you must select a storage size for the new appliance that is suitable for the database size.

7.0 uses an embedded vSphere Lifecycle Manager service that allows you to perform centralized and simplified lifecycle management of clusters with ESXi 7.0 hosts. vSphere Lifecycle Manager in vSphere 7.0 includes the functionality that Update Manager provided in earlier vSphere releases for host upgrade and patching operations, as well as upgrade of virtual machine hardware and VMware Tools.

If you are upgrading a appliance or migrating a that use an external Update Manager instance that runs on Windows, in vSphere 7.0 the external Update Manager instance is migrated to the embedded vSphere Lifecycle Manager extension service of the new, upgraded appliance.

If you are upgrading a appliance that uses an embedded VMware Update Manager instance, in vSphere 7.0 the embedded VMware Update Manager instance is upgraded to the embedded vSphere Lifecycle Manager extension service of the new upgraded appliance. The embedded VMware vSphere Update Manager Extension uses the embedded PostgreSQL database. Before the upgrade, you must run the Migration Assistant on the source Update Manager instance.

For information about the software included in the 7.0, see *vCenter Server Installation and Setup*.

Note: vCenter Server deployments using an external Platform Services Controller will not be supported in a future vSphere release. For more information, see Decommission the Platform Services Controller and Knowledge Base article KB 60229. For topologies with external Platform Services Controller instances, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the upgrade. To learn more about converging a vCenter Server deployment using an external Platform Services Controller into a vCenter Server appliance, see Knowledge Base article KB 68137.

The installer contains executable files for both GUI and CLI upgrades which you can use alternatively.

- The GUI upgrade is a two stage process. The first stage is a Deployment wizard that deploys the OVA file of the new appliance on the target ESXi host or vCenter Server instance. After the OVA deployment finishes, you are redirected to the second stage of the process that sets up and transfers the services and configuration data from the old appliance to the newly deployed appliance.
- The CLI upgrade method involves running a CLI command against a JSON file that you previously prepared. The CLI installer parses the configuration parameters and their values from the JSON file and generates an OVF Tool command that deploys the new appliance. The OVF Tool command also transfers services and configuration data and from the old appliance to the new appliance.

For information about the and Platform Services Controller appliance upgrade requirements, see System Requirements for the vCenter Server Appliance.

Important: If the appliance that you are upgrading is configured in a mixed IPv4 and IPv6 environment, only the IPv4 settings are preserved. for information on the transfer of networking configuration settings for mixed mode IPv4 and IPv6 deployments, see Mixed IPv4 and IPv6 Upgrade and Migration.

If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not shown. After the upgrade, you can manually connect the appliance to the original non-ephemeral

distributed virtual port group. This is not a limitation when deploying the appliance through a vCenter Server, and you can deploy to ephemeral or non-ephemeral distributed virtual port groups.

To upgrade appliance version 6.0 or earlier, you must first upgrade to version 6.5 or 6.7 and then upgrade to version 7.0. For information about upgrading appliance 6.0 to version 6.5, see the *VMware vSphere 6.5* documentation. For information about upgrading appliance 6.0 to version 6.7, see the *VMware vSphere 6.7* documentation. For information on the upgrade compatibility of vCenter Server, see the VMware Compatibility Guide.

For information about deploying the , see *vCenter Server Installation and Setup*.

For information about configuring the , see *vCenter Server Configuration*.

About the Upgrade Process of the vCenter Server Appliance

You can upgrade the appliance from version 6.5 or 6.7 to version 7.0.

Important: If your current appliance is version 6.0 or earlier, you must upgrade to version 6.5 or 6.7 before upgrading to version 7.0.

Important: In environments with multiple instances of appliance, you cannot perform parallel upgrades. Each instance must be upgraded separately. The reason for this is that VMware Directory Services (`vmdird`) encounters replication problems with single-sign on and certificate information.

When you run the GUI or CLI upgrade, the process includes:

1. Deploying a new 7.0 with a temporary network configuration.
   If you are upgrading a , you must select a deployment size for the new appliance that is suitable for your vSphere environment size. You must also select a storage size for the new appliance that is suitable for the database. If the source uses an external database, see Determine the Oracle Database Size and the Storage Size for the New Appliance.
2. Exporting the services and configuration data from the source appliance of version 6.5 or 6.7 that you want to upgrade.
   You must select the data types that you want to transfer to the new appliance.
   If you are upgrading a appliance that uses an external Update Manager instance, you must ensure that the Migration Assistant is running on the Update Manager computer. Migration Assistant facilitates the export of the Update Manager configuration and database.
3. Transferring the exported data to the newly deployed appliance
   If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and do not appear as options during the upgrade. After the upgrade, you can manually connect the appliance to the original non-ephemeral distributed virtual port group. This process is not a limitation when deploying the appliance through a vCenter Server, and you can deploy to ephemeral or non-ephemeral distributed virtual port groups.
   If you are upgrading a appliance that uses a Update Manager instance, the Update Manager instance is migrated to the vSphere Lifecycle Manager of the new upgraded appliance. To learn more about vSphere Lifecycle Manager, see the *Managing Host and Cluster Lifecycle* documentation.
4. If you are upgrading a appliance that uses an external Platform Services Controller, it is converted to a instance with those services embedded in the appliance.
   The new appliance contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into during the upgrade.
5. Powering off the source appliance. The new upgraded appliance assumes the network configuration of the source appliance.

- For the new appliance requirements, see System Requirements for the vCenter Server Appliance.
- For the appliance upgrade preparation, see Preparing to Upgrade the vCenter Server Appliance.
- For the appliance upgrade procedures, see Upgrading the vCenter Server Appliance.

- For the appliance post-upgrade procedures, see After Upgrading or Migrating vCenter Server.

System Requirements for the vCenter Server Appliance

You can deploy the vCenter Server appliance on an ESXi host 6.5 or later, or on a vCenter Server instance 6.5 or later. Your system must also meet specific software and hardware requirements.

When you use Fully Qualified Domain Names, verify that the client machine from which you are deploying the appliance and the network on which you are deploying the appliance use the same DNS server.

Before you deploy the appliance, synchronize the clocks of the target server and all vCenter Server instances on the vSphere network. Unsynchronized clocks might result in authentication problems and can cause the installation to fail or prevent the appliance services from starting. See Synchronizing Clocks on the vSphere Network.

Hardware Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance, you can select to deploy an appliance that is suitable for the size of your vSphere environment. The option that you select determines the number of CPUs and the amount of memory for the appliance.

Hardware Requirements for the vCenter Server Appliance

The hardware requirements for a vCenter Server appliance depend on the size of your vSphere inventory.

Table 58: Hardware Requirements for a vCenter Server Appliance

	Number of vCPUs	Memory
Tiny environment (up to 10 hosts or 100 virtual machines)	2	12 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	4	19 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	8	28 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	16	37 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	24	56 GB

Note: If you want to add an ESXi host with more than 512 LUNs and 2,048 paths to the vCenter Server inventory, you must deploy a vCenter Server appliance for a large or x-large environment.

Storage Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance, the ESXi host or DRS cluster on which you deploy the appliance must meet minimum storage requirements. The required storage depends not only on the size of the vSphere environment and the storage size, but also on the disk provisioning mode.

Storage Requirements for the vCenter Server Appliance

The storage requirements are different for each vSphere environment size and depend on your database size requirements.

Table 59: Storage Requirements for a vCenter Server Appliance

	Default Storage Size	Large Storage Size	X-Large Storage Size
Tiny environment (up to 10 hosts or 100 virtual machines)	579 GB	1992 GB	4279 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	694 GB	2046 GB	4304 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	908 GB	2140 GB	4468 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	1358 GB	1958 GB	4518 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	2283 GB	2383 GB	4620 GB

Note: The storage requirements include the requirements for the vSphere Lifecycle Manager that runs as a service in the vCenter Server appliance.

Related Links

Determine the Oracle Database Size and the Storage Size for the New Appliance on page 1322

Before upgrading a vCenter Server appliance or migrating a vCenter Server on Windows that uses an external Oracle database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new vCenter Server appliance database using an embedded PostgreSQL database.

Software Requirements for the vCenter Server Appliance

The VMware vCenter Server appliance can be deployed on ESXi 6.5 hosts or later, or on vCenter Server instances 6.5 or later.

You can deploy the vCenter Server appliance using the GUI or CLI installer. You run the installer from a network client machine that you use to connect to the target server and deploy the appliance on the server. You can connect directly to an ESXi 6.5 host on which to deploy the appliance. You can also connect to a vCenter Server 6.5 instance to deploy the appliance on an ESXi host or DRS cluster that resides in the vCenter Server inventory.

For information about the requirements for network client machine, see System Requirements for the vCenter Server Installer.

Required Ports for vCenter Server

The vCenter Server system must be able to send data to every managed host and receive data from the vSphere Client. To enable migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other through predetermined TCP and UDP ports.

vCenter Server is accessed through predetermined TCP and UDP ports. If you manage network components from outside a firewall, you might be required to reconfigure the firewall to allow access on the appropriate ports. For the list of all supported ports and protocols in vSphere, see the VMware Ports and Protocols Tool™ at https://ports.broadcom.com.

During installation, if a port is in use or is blocked using a denylist, the vCenter Server installer displays an error message. You must use another port number to proceed with the installation. There are internal ports that are used only for inter-process communication.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from vCenter Server. If a built-in firewall exists between any of these elements, the installer opens the ports during the installation or upgrade process. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

To configure the vCenter Server system to use a different port to receive vSphere Client data, see the *vCenter Server and Host Management* documentation.

DNS Requirements for the vCenter Server Appliance

When you deploy the vCenter Server appliance with a static IP address, you ensure that in case of system restart, the IP address of the appliance remains the same.

Before you deploy the vCenter Server appliance with a static IP address, you must verify that this IP address has a valid internal domain name system (DNS) registration.

When you deploy the vCenter Server appliance, the installation of the web server component that supports the vSphere Client fails if the installer cannot look up the fully qualified domain name (FQDN) for the appliance from its IP address. Reverse lookup is implemented using PTR records.

If you plan to use an FQDN for the appliance system name, you must verify that the FQDN is resolvable by a DNS server, by adding foward and reverse DNS A records.

You can use the `nslookup` command to verify that the DNS reverse lookup service returns an FQDN when queried with the IP address and to verify that the FQDN is resolvable.

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

If you use DHCP instead of a static IP address for the vCenter Server appliance, verify that the appliance name is updated in the domain name service (DNS). If you can ping the appliance name, the name is updated in DNS.

Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Client instances. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and vSphere Client.

vSphere Client Software Requirements

Use of the vSphere Client requires a supported web browser.

VMware has tested and supports the following guest operating systems and browser versions for the vSphere Client.

Supported Guest Operating Systems	• Windows 32-bit and 64-bit • Mac OS
Supported Browser Versions	• Google Chrome 89 or later • Mozilla Firefox 80 or later • Microsoft Edge 90 or later **Note:** Later versions of these browsers are likely to work, but have not been tested.

Preparing to Upgrade the vCenter Server Appliance

Before you upgrade the vCenter Server appliance, you must download the vCenter Server installer ISO file and mount it to a network virtual machine or physical server from which you want to perform the upgrade.

The computer from which you upgrade the appliance must run on a Windows, Linux, or Mac operating system that meets the operating system requirements. See System Requirements for the vCenter Server Installer.

Before upgrading a vCenter Server appliance, you must prepare the ESXi hosts in the inventory.

Before upgrading a vCenter Server deployment using an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the upgrade. See Knowledge Base article KB 68137.

If the vCenter Server appliance uses an external Oracle database, you must determine the size of the existing database.

If vCenter Server appliance uses an external Update Manager instance, you must run the Migration Assistant on the computer running Update Manager.

System Requirements for the vCenter Server Installer

You can run the vCenter Server GUI or CLI installer from a network client machine that is running on a Windows, Linux, or Mac operating system of a supported version.

To ensure optimal performance of the GUI and CLI installers, use a client machine that meets the minimum hardware requirements.

Table 60: System Requirements for the GUI and CLI Installers

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
Windows	• Windows 8, 8.1, 10 • Windows 2012 x64 bit • Windows 2012 R2 x64 bit • Windows 2016 x64 bit • Windows 2019 x64	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC
Linux	• SUSE 15 • Ubuntu 16.04 and 18.04	4 GB RAM, 1 CPU having 2 cores with 2.3 GHz, 16 GB hard disk, 1 NIC **Note:** The CLI installer requires 64-bit OS.
Mac	• macOS v10.13, 10.14, 10.15 • macOS High Sierra, Mojave, Catalina	8 GB RAM, 1 CPU having 4 cores with 2.4 GHz, 150 GB hard disk, 1 NIC

Note: For client machines that run on Mac 10.13 or later, concurrent GUI deployments of multiple appliances are unsupported. You must deploy the appliances in a sequence.

Note: Visual C++ redistributable libraries need to be installed to run the CLI installer on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa-cli-installer/win32/vcredist` directory.

Note: Deploying the vCenter Server appliance with the GUI requires a minimum resolution of 1024x768 to properly display. Lower resolutions can truncate the UI elements.

Download and Mount the vCenter Server Installer

VMware releases the vCenter Server appliance ISO image, which contains GUI and CLI installers for the vCenter Server appliance.

- Access to Broadcom Support.
- Verify that your client machine meets the system requirements for the vCenter Server installer. See System Requirements for the vCenter Server Installer.

With the GUI and CLI executable files that are included in the vCenter Server installer, you can:

- Deploy the vCenter Server appliance.
- Upgrade the vCenter Server appliance.
- Converge older versions of vCenter Server with an external Platform Services Controller to the current version of vCenter Server.
- Restore a vCenter Server appliance from a file-based backup.

1. Log in to Broadcom Support Portal.
2. Download the vCenter Server appliance ISO image.

   See the Knowledge Base article.
3. Download the vCenter Server appliance ISO image.
4. Confirm that the md5sum is correct by using an MD5 checksum tool.
5. Mount the ISO image to the client machine from which you want to deploy, upgrade, migrate, or restore the appliance.

   Note: ISO mounting software that does not allow more than eight directory levels, for example, MagicISO Maker on Windows, is unsupported.

   For Linux OS and Mac OS, Archive Manager is unsupported.

   For Mac OS, you can use DiskImageMounter.
   For Ubuntu 14.04, you can use Disk Image Mounter.
   For SUSE 12 OS, you can use the terminal.

   ```
   $ sudo mkdir mount_dir
   $ sudo mount -o loop VMware-vCSA-all-version_number-build_number.iso mount_dir
   ```

   Important: Due to a security change in MacOS Catalina, you must modify the security settings on your computer until the vCenter Server deployment completes. If you attempt to run the installer under MacOS Catalina without modifying the security settings, the vCenter Server installer reports the error:`ovftool cannot be opened because the developer cannot be verified.` For more information, see KB 79416.

Open the `readme.txt` file and review the information about the other files and directories in the vCenter Server appliance ISO image.

Synchronizing Clocks on the vSphere Network

Verify that all components on the vSphere network have their clocks synchronized. If the clocks on the physical machines in your vSphere network are not synchronized, SSL certificates and SAML tokens, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server`vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause the first boot of a component in your environment to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server is not synchronized with NTP or PTP.

Similarly, issues can arise if the destination vCenter Server migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server instance.

- The target ESXi host where the destination vCenter Server is to be deployed is synchronized to NTP or PTP.
- The ESXi host running the source vCenter Server is synchronized to NTP or PTP.
- When upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, if the vCenter Server appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP or PTP.
- If you are upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, verify that the source vCenter Server or vCenter Server appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the VMware knowledge base article at https://kb.vmware.com/s/article/1318.

To synchronize ESXi clocks with an NTP or a PTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see topic *Edit the Time Configuration of an ESXi Host in the VMware Host Client* in the *vSphere Single Host Management - VMware Host Client* documentation.

To learn how to change time synchronization settings for vCenter Server, see topic *Configure the System Time Zone and Time Synchronization Settings* in the *vCenter Server Configuration* documentation.

To learn how to edit the time configuration for a host by using the vSphere Client, see topic *Editing the Time Configuration Settings of a Host* in the *vCenter Server and Host Management* documentation.

Transferring Data After Upgrade or Migration

Typically, data transfer happens as part of the upgrade downtime. However, in some scenarios you can choose to transfer a part of the data after upgrade or migration to minimize the downtime.

Transfer of data after upgrade or migration is supported in the following scenarios:

- Migrating vCenter Server for Windows to vCenter Server Appliance
- Upgrading vCenter Server appliance with external database

  Note: You can only transfer data from external database to the embedded PostgreSQL database in the background after upgrade or migration. Transferring data from an embedded PostgreSQL database to another embedded PostgreSQL database after upgrade or migration is not supported.

You can transfer the minimum amount of data necessary to be operational during the upgrade. Later, you can transfer the remaining data from the external database to the embedded PostgreSQL database in the background, preserving your deployment's historical event and performance data.

You can transfer historical data after the upgrade or migration from the following vCenter Server versions using external databases to the embedded PostgreSQL database within the vCenter Server appliance.

Table 61: vCenter Server Database Support for Data Transfer After Upgrade or Migration

vCenter Server Versions	Databases	Support for Data Transfer After Upgrade or Migration
vCenter Server appliance 6.5	Embedded PostgreSQL database Not Supported	
vCenter Server for Windows 6.5	External Oracle or MS SQL database	Supported
	Embedded PostgreSQL database	Not supported
vCenter Server appliance 6.7	Embedded PostgreSQL database	Not supported

vCenter Server Versions	Databases	Support for Data Transfer After Upgrade or Migration
vCenter Server for Windows 6.7	External Oracle or MS SQL database	Supported
	Embedded PostgreSQL database	Not supported

You can transfer the following types of data from an external database to the embedded PostgreSQL database in use by version 7.0 of the vCenter Server appliance.

Configuration data
The minimum type of data you must transfer from your existing vCenter Server appliance external database to upgrade or migrate to a functioning vCenter Server appliance. This data can be transferred in a reasonably short amount of time, minimizing downtime during the upgrade to vCenter Server7.0.

Configuration and historical data
In addition to the configuration data, you can choose to transfer historical data such as usage statistics, events, and tasks. The vCenter Server installer gives you the option to copy both the configuration and historical data at one time, or to copy only the configuration data during the upgrade process. You can then choose to copy the historical data in the background after you start your new vCenter Server.

Attention: If you choose to copy all data at one time, you cannot start vCenter Server until all the data has been transferred to the embedded PostgreSQL database within vCenter Server7.0.

Configuration, historical, and performance metrics data
The largest amount of data you can choose to transfer to vCenter Server. You can copy only the configuration data during the upgrade process, and then copy the historical and performance data in the background after the upgrade or migration to vCenter Server7.0 finishes.

Monitor and Manage Historical Data Migration

You can monitor and manage the background migration of historical data using the vCenter Server Management Interface. You can perform the following data management tasks:

- Monitor the progress of the data migration.
- Pause the data import.
- Cancel the data import.

  Important: If you cancel the data import, the historical data is not imported to the embedded PostgreSQL database. If you cancel the data import operation, you cannot recover the data. If you do cancel the data import, and want to import the historical data later, you must restart the upgrade or migration process from Stage 1 of the GUI installer.

See Monitor and Manage Historical Data Migration.

Prepare ESXi Hosts for vCenter Server Appliance Upgrade

Before upgrading to vCenter Server7.0, you must prepare your ESXi hosts.

To upgrade vCenter Server appliance, your ESXi hosts must meet the requirements for upgrade.

- ESXi hosts must be at version 6.5 or later. For information on ESXi compatibility, see the VMware Compatibility Guide.

- Your source and target ESXi hosts must not be in lockdown or maintenance mode, and not part of fully automated DRS clusters.
- Review your environment's Certificate Authority (CA) signed SSL certificates. To learn about manually reviewing CA signed SSL certificates in a vSphere environment, see Knowledge Base article KB 2111411.

1. If you have Custom or Thumbprint certificates, see Host Upgrades and Certificates to determine your preparatory steps.
2. If you have vSphere HA clusters, SSL certificate checking must be enabled.

   If certificate checking is not enabled when you upgrade ESXi hosts, vSphere HA fails to configure on the hosts.

   a) Select the vCenter Server appliance instance in the vSphere Client inventory tree.
   b) Select the **Configure** tab, and then under **Settings** select **General**.
   c) Click **Edit**.
   d) Select **SSL settings**.

      Verify that **vCenter Server requires verified host SSL certificates** is selected.

Your ESXi hosts are ready for the vCenter Server appliance upgrade.

Host Upgrades and Certificates

If you upgrade an ESXi host to ESXi 6.5 or later, the upgrade process replaces the self-signed (thumbprint) certificates with VMCA-signed certificates. If the ESXi host uses custom certificates, the upgrade process retains those certificates even if those certificates are expired or invalid.

The recommended upgrade workflow depends on the current certificates.

Host Provisioned with Thumbprint Certificates	If your host is currently using thumbprint certificates, it is automatically assigned VMCA certificates as part of the upgrade process. **Note:** You cannot provision legacy hosts with VMCA certificates. You must upgrade those hosts to ESXi 6.5 or later.
Host Provisioned with Custom Certificates	If your host is provisioned with custom certificates, usually third-party CA-signed certificates, those certificates remain in place during upgrade. Change the certificate mode to **Custom** to ensure that the certificates are not replaced accidentally during a certificate refresh later. **Note:** If your environment is in VMCA mode, and you refresh the certificates from the vSphere Client, any existing certificates are replaced with certificates that are signed by VMCA. Going forward, vCenter Server monitors the certificates and displays information, for example, about certificate expiration, in the vSphere Client.
Hosts Provisioned with Auto Deploy	Hosts that are being provisioned by Auto Deploy are always assigned new certificates when they are first booted with ESXi 6.5 or later software. When you upgrade a host that is provisioned by Auto Deploy, the Auto Deploy server generates a certificate signing request (CSR) for the host and submits it to VMCA. VMCA stores the signed certificate for the host. When the Auto Deploy server provisions the host, it retrieves the certificate from VMCA and includes it as part of the provisioning process. You can use Auto Deploy with custom certificates.

Change the Certificate Mode

Use VMware Certificate Authority (VMCA) to provision certificates of the ESXi hosts in your environment unless corporate policy requires that you use custom certificates. To use custom certificates with a different root CA, you can edit the vCenter Servervpxd.certmgmt.mode advanced option. After the change, the hosts are no longer automatically provisioned with VMCA certificates when you refresh the certificates. You are responsible for the certificate management in your environment.

You can use the vCenter Server advanced settings to change to thumbprint mode or to custom CA mode. Use thumbprint mode only as a fallback option.

1. In the vSphere Client, select the vCenter Server system that manages the hosts.
2. Click **Configure**, and under Settings, click **Advanced Settings**.
3. Click **Edit Settings**.
4. Click the **Filter** icon in the Name column, and in the Filter box, enter `vpxd.certmgmt` to display only certificate management parameters.
5. Change the value of vpxd.certmgmt.mode to **custom** if you intend to manage your own certificates, and to **thumbprint** if you temporarily want to use thumbprint mode, and click **Save**.
6. Restart the vCenter Server service.

   See the *vCenter Server Configuration* documentation for information about restarting services.

Determine the Oracle Database Size and the Storage Size for the New Appliance

Before upgrading a vCenter Server appliance or migrating a vCenter Server on Windows that uses an external Oracle database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new vCenter Server appliance database using an embedded PostgreSQL database.

You must have the vCenter Server database login credentials.

You run scripts to determine the Oracle core table size, the events and tasks table size, and the statistics table size. The Oracle core table corresponds to the database (`/storage/db`) partition of the PostgreSQL database. The Oracle events and tasks and statistics tables correspond to the statistics, events, alarms, and tasks (`/storage/seat`) partition of the PostgreSQL database.

During the upgrade of the appliance, you must select a storage size for the new appliance that is at least twice the size of the Oracle tables size.

During the upgrade of the appliance, you can select the types of data to transfer to the new appliance. To minimize upgrade time and storage requirements for the new appliance, you can choose to transfer only the configuration data.

1. Log in to a SQL*Plus session with the vCenter Server database user.
2. Determine the core table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
  FROM   user_segments s
  WHERE  (s.segment_name,s.segment_type)
               IN (SELECT seg_name, seg_type FROM
                        (SELECT t.table_name seg_name, t.table_name tname,
                          'TABLE' seg_type
                          FROM   user_tables t
                         UNION
                         SELECT i.index_name, i.table_name,
                         'INDEX'
```

```
                        FROM   user_indexes i
                      ) ti
                WHERE  (ti.tname LIKE 'VPX_%'
                        OR ti.tname LIKE 'CL_%'
                        OR ti.tname LIKE 'VDC_%')
                   AND ti.tname NOT LIKE 'VPX_SAMPLE_TIME%'
                   AND ti.tname NOT LIKE 'VPX_HIST_STAT%'
                   AND ti.tname NOT LIKE 'VPX_TOPN%'
                   AND ti.tname NOT LIKE 'VPX_SDRS_STATS_VM%'
                   AND ti.tname NOT LIKE 'VPX_SDRS_STATS_DATASTORE%'
                   AND ti.tname NOT LIKE 'VPX_TASK%'
                   AND ti.tname NOT LIKE 'VPX_EVENT%'
                   AND ti.tname NOT LIKE 'VPX_PROPERTY_BULLETIN%');
```

The script returns the database storage size in MB.

3. Determine the events and tasks table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                      (SELECT t.table_name seg_name, t.table_name tname,
                        'TABLE' seg_type
                        FROM   user_tables t
                       UNION
                       SELECT i.index_name, i.table_name,
                       'INDEX'
                        FROM   user_indexes i
                      ) ti
                   WHERE
                      ti.tname LIKE 'VPX_TASK%'
                   OR ti.tname LIKE 'VPX_EVENT%');
```

The script returns the events and tasks storage size in MB.

4. Determine the statistics table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                      (SELECT t.table_name seg_name, t.table_name tname,
                        'TABLE' seg_type
                        FROM   user_tables t
                       UNION
                       SELECT i.index_name, i.table_name,
                       'INDEX'
                        FROM   user_indexes i
                      ) ti
                   WHERE
                      ti.tname LIKE 'VPX_SAMPLE_TIME%'
                   OR ti.tname LIKE 'VPX_TOPN%'
                   OR ti.tname LIKE 'VPX_TASK%'
                   OR ti.tname LIKE 'VPX_EVENT%'
```

```
                OR ti.tname LIKE 'VPX_HIST_STAT%');
```

The script returns the statistics storage size in MB.

5. Calculate the minimum storage size for the new appliance that you are going to deploy during the upgrade.
   a) The size of the database (`/storage/db`) partition of the embedded PostgreSQL database must be at least twice the size of the Oracle core table returned in 2.
   b) The size of the statistics, events, alarms, and tasks (`/storage/seat`) partition of the embedded PostgreSQL database must be at least twice the sum of the sizes of the Oracle events and tasks and statistics tables returned in 3 and 4.

   For example, if the Oracle core table is 100 MB, the events and tasks table is 1,000 MB, and the statistics table is 2,000 MB, then the Postgres `/storage/db` partition must be at least 200 MB and the `/storage/seat` partition must be at least 6,000 MB.

Related Links

Storage Requirements for the vCenter Server Appliance on page 1246

When you deploy the vCenter Server appliance, the ESXi host or DRS cluster on which you deploy the appliance must meet minimum storage requirements. The required storage depends not only on the size of the vSphere environment and the storage size, but also on the disk provisioning mode.

Download and Run VMware Migration Assistant on the Source Update Manager Machine

During the upgrade of a vCenter Server appliance that uses an external Update Manager, the Migration Assistant must be running on the source Update Manager machine. This procedure describes how to download and run the Migration Assistant manually before the upgrade.

- Download and Mount the vCenter Server Installer.
- Log in to the source Update Manager machine as an administrator.

The Migration Assistant facilitates the migration of the Update Manager server and database to the new upgraded vCenter Server appliance. The Migration Assistant uses port 9123 by default. If port 9123 is used by another service on your Update Manager machine, the Migration Assistant automatically finds a different free port to use.

Alternatively, if you plan to upgrade the vCenter Server appliance by using the CLI installer, you can add the `source.vum section` section and `run.migration.assistant` subsection to your JSON template. For information about the CLI upgrade configuration parameters, see Upgrade Configuration Parameters for CLI Upgrade of vCenter Server Appliance .

1. From the vCenter Server appliance installer package, copy the `migration-assistant` directory to the source Update Manager machine.
2. From the `migration-assistant` directory, double-click `VMware-Migration-Assistant.exe` and the provide the vCenter Single Sign-On administrator password.
3. Leave the Migration Assistant window open until the upgrade of the vCenter Server appliance finishes.

When the pre-checks are finished and any errors are addressed, your source Update Manager system is ready for the upgrade.

CAUTION: Closing the Migration Assistant window causes the upgrade process to stop.

Prerequisites for Upgrading the vCenter Server Appliance

To ensure a successful upgrade of the vCenter Server appliance, you must perform the following required tasks and pre-checks before beginning the upgrade process.

General Prerequisites

- Download and Mount the vCenter Server Installer.

- Verify that the clocks of all computers on the vSphere network are synchronized. See Synchronizing Clocks on the vSphere Network.

Target System Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the vCenter Server Appliance.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on an ESXi host managed by vCenter Server, review the Distributed Resource Scheduler (DRS) settings on the cluster. Ensure that the DRS settings for the cluster on which the target ESXi host resides are not configured for Full Automation. Set the Automation Level to Manual or Partially Automated. This Automation Level ensures that the target ESXi host does not reboot during the upgrade process.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster is not fully automated.

Source System Prerequisites

- Ensure that DRS is set to manual for the cluster temporarily so that the VMs for the Source and Target do not get moved during the upgrade.
- Verify that port 22 is open on the vCenter Server appliance that you want to upgrade. The upgrade process establishes an inbound SSH connection to download the exported data from the source vCenter Server appliance.
- If you are upgrading a vCenter Server appliance that is configured with an external Update Manager, run the Migration Assistant on the source Update Manager computer.

  For a GUI upgrade, you must run Migration Assistant manually. See Download and Run VMware Migration Assistant on the Source Update Manager Machine.

  For a CLI upgrade, you can run Migration Assistant manually or automatically. To run Migration Assistant automatically, add the `source.vum section` section and `run.migration.assistant` subsection to your JSON template. See Upgrade Configuration Parameters for CLI Upgrade of vCenter Server Appliance .
- Verify that port 443 is open on the source ESXi host on which the appliance that you want to upgrade resides. The upgrade process establishes an HTTPS connection to the source ESXi host to verify that the source appliance is ready for upgrade and to set up an SSH connection between the new and the existing appliance.

  Note: When upgrading, the temporary vCenter Server instance requires the same access rights as the permanent vCenter Server instance to port 443. Ensure that any firewalls in your environment allow both the temporary and permanent vCenter Server instances to access port 443.
- Verify that you have sufficient free disk space on the appliance that you want to upgrade so that you can accommodate the data for the upgrade.
- Create an image-based backup (snapshot) of the vCenter Server appliance you are upgrading as a precaution in case there is a failure during the upgrade process. If you are upgrading a vCenter Server appliance with an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the upgrade. See Knowledge Base article KB 68137.

  Important: To take a pre-upgrade image-based backup in an Enhanced Linked Mode environment, power off all the vCenter Server and Platform Services Controller nodes in your environment, and back up each node. After you have taken backups of all the nodes, you can restart them and proceed with the upgrade procedure.

  If the upgrade fails, delete the newly deployed vCenter Server appliance, and restore the vCenter Server and Platform Services Controller nodes from their respective backups. You must restore all the nodes in the environment from their backups. Failing to do so will cause the replication partners to be out of synchronization with the restored node.

  To learn about image-based back, see "Image-Based Backup and Restore of a vCenter Server Environment" in *vCenter Server Installation and Setup*.

- If you use an external database, determine the database size and the minimum storage size for the new appliance. See Determine the Oracle Database Size and the Storage Size for the New Appliance.
- If your deployment uses an external database, you must back up the external vCenter Server appliance database.

Network Prerequisites

- Verify that the new appliance can connect to the source ESXi host or vCenter Server instance on which resides the appliance that you want to upgrade.
- If you plan to assign a static IP address and an FQDN as a system name in the temporary network settings of the appliance, verify that you have configured the forward and reverse DNS records for the IP address.
- If you plan to assign a DHCP IP address in the temporary network settings of the new vCenter Server appliance, verify that the ESXi host on which you want to deploy the new appliance is in the same subnet as the ESXi host on which the existing vCenter Server appliance runs.
- If you plan to assign a DHCP IPv4 address in the temporary network settings of the new vCenter Server appliance, verify that the ESXi host on which you want to deploy the new appliance is connected to at least one network that is associated with a port group which accepts MAC address changes. Consider the default security policy of a distributed virtual switch, which is to reject MAC address changes. For information about how to configure the security policy for a switch or port group, see *vSphere Networking*.

GUI Upgrade of the vCenter Server Appliance

You can use the GUI installer to perform an interactive upgrade of a vCenter Server appliance.

To perform the GUI upgrade, download the vCenter Server appliance installer on a network client machine, run the Upgrade Wizard from the client machine, and provide the inputs for the deployment and setup of the new upgraded appliance.

Note: When you upgrade vCenter Server 6.5 or 6.7 with an external Platform Services Controller to vCenter Server7.0, the upgrade process converges the external Platform Services Controller into the new vCenter Server appliance. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to upgrade and use an external Platform Services Controller.

After successfully upgrading your environment to vCenter Server7.0, the pre-existing Platform Services Controller will be powered off, and you can remove it from your vSphere inventory. See Decommission the Platform Services Controller.

The GUI upgrade process includes a series of two stages.

Figure 35: Stage 1 - OVA Deployment

The first stage walks you through the deployment wizard to get the deployment type of the source appliance that you want to upgrade and configure the new appliance settings. During this stage, you deploy the new appliance with temporary network settings. This stage finishes the deployment of the OVA file on the target server with the same deployment type as the source appliance and the appliance settings that you provide.

As an alternative to performing the first stage of the upgrade with the GUI installer, you can deploy the OVA file of the new vCenter Server appliance using the vSphere Client or VMware Host Client. To deploy the OVA file on an ESXi host or vCenter Server instance 6.5 or later, you can also use the vSphere Client. After the OVA deployment, you must log in to the appliance management interface of the newly deployed appliance to proceed with the second stage of the upgrade process.

Figure 36: Stage 2 - Appliance Setup

The second stage walks you through the setup wizard to select the data types to transfer from the old to the new appliance. The new appliance uses the temporary network settings until the data transfer finishes. After the data transfer finishes, the new appliance assumes the network settings of the old appliance. This stage finishes the data transfer, starts the services of the new upgraded appliance, and powers off the old appliance.

As an alternative to performing the second stage of the upgrade with the GUI installer, you can log in to the vCenter Server Management Interface of the newly deployed appliance, https://*FQDN_or_IP_address*:5480.

Required Information for Upgrading a vCenter Server Appliance 6.5 or 6.7

The GUI upgrade wizard prompts you for information about the vCenter Server appliance that you want to upgrade, deployment information for the new vCenter Server appliance 7.0. It is a best practice to keep a record of the values that you enter.

You can use this worksheet to record the information that you need for upgrading a vCenter Server appliance with an embedded Platform Services Controller or a vCenter Server appliance with an external Platform Services Controller.

Table 62: Required Information During Stage 1 of the Upgrade

Required for Upgrade of	Required Information	Default	Your Entry
All deployment types	FQDN or IP address of the source appliance that you want to upgrade.	-	
	HTTPS port of the source appliance.	443	
	vCenter Single Sign-On administrator user name of the source appliance. **Important:** The user must be administrator@*your_domain_name*.	administrator@vsphere.local	
	Password of the vCenter Single Sign-On administrator user.	-	
	Password of the root user of the source appliance	-	
All deployment types	FQDN or IP address of the source server on which resides that appliance that you want to upgrade. The source server can be either an ESXi host or a vCenter Server instance. **Note:** The source server cannot be the vCenter Server appliance that you want to upgrade. In such cases, use the source ESXi host.	-	
	HTTPS port of the source server.	443	
	User name with administrative privileges on the source server. • If your source server is an ESXi host, use root. • If your source server is a vCenter Server instance, use *user_name*@*your_domain_name*, for example, administrator@vsphere.local.	-	

Required for Upgrade of	Required Information	Default	Your Entry
	Password of the user with administrative privileges on the source server.	-	
All deployment types	FQDN or IP address of the target server on which you want to deploy the new appliance. The target server can be either an ESXi host or a vCenter Server instance. **Note:** The target server cannot be the vCenter Server appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	-	
	HTTPS port of the target server.	443	
	User name with administrative privileges on the target server • If your target server is an ESXi host, use root. • If your target server is a vCenter Server instance, use *user_name*@*your_domain_name*, for example, administrator@vsphere.local.	-	
	Password of the user with administrative privileges on the target server.	-	
All deployment types Only if your target server is a vCenter Server instance.	Data center from the vCenter Server inventory on which you want to deploy the new appliance. Optionally you can provide a data center folder.	-	
	ESXi host or DRS cluster from the data center inventory on which you want to deploy the new appliance .	-	
All deployment types	The virtual machine name for the new appliance. • Must not contain a percent sign (%), backslash (\), or forward slash (/). • Must be no more than 80 characters in length.	VMware vCenter Server Appliance	
All deployment types	Password for the root user of the appliance operating system. • Must contain only the lower ASCII character set without spaces. • Must be at least 8 characters, but no more than 20 characters in length. • Must contain at least one uppercase letter. • Must contain at least one lowercase letter. • Must contain at least one number. • Must contain at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!).	-	
• vCenter Server appliance 6.5 with an embedded Platform Services Controller • vCenter Server appliance 6.7 with an external Platform Services Controller	Deployment size of the new vCenter Server appliance for your vSphere environment. • Tiny Deploys an appliance with 2 CPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines.	The size of the source vCenter Server appliance and Platform Services Controller determines the default deployment size. Using this information,	

Required for Upgrade of	Required Information	Default	Your Entry
• vCenter Server appliance 6.5 with an embedded Platform Services Controller • vCenter Server appliance 6.7 with an external Platform Services Controller	• Small Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines. • Medium Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines. • Large Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines. • X-Large Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,000 hosts or 35,000 virtual machines.	the upgrade installer calculates the best size to use for your environment, which might be the same as your existing deployment, or calculated to the next largest size.	
• vCenter Server appliance 6.5 with an external Platform Services Controller • vCenter Server appliance 6.7 with an external Platform Services Controller	Storage size of the new vCenter Server appliance for your vSphere environment. Increase the default storage size if you want larger volume for SEAT data (stats, events, alarms, and tasks). **Note:** Consider the database size of the appliance that you want to upgrade and the types of the data that you want transfer to the new appliance. For an external database, see Determine the Oracle Database Size and the Storage Size for the New Appliance. • Default For tiny deployment size, deploys the appliance with 415 GB of storage. For small deployment size, deploys the appliance with 480 GB of storage. For medium deployment size, deploys the appliance with 700 GB of storage. For large deployment size, deploys the appliance with 1065 GB of storage. For x-large deployment size, deploys the appliance with 1805 GB of storage.	Default **Note:** The sizing algorithm in use by the upgrade installer might select a larger storage size for your environment. Items that might affect the storage size selected by the installer include modifications to the vCenter Server appliance disks (for example, changing the size of the logging partition), or databases having a database table that the installer determines to be exceptionally large and requiring additional hard disk space.	

Required for Upgrade of	Required Information	Default	Your Entry
	• Large For tiny deployment size, deploys the appliance with 1490 GB of storage. For small deployment size, deploys the appliance with 1535 GB of storage. For medium deployment size, deploys the appliance with 1700 GB of storage. For large deployment size, deploys the appliance with 1765 GB of storage. For x-large deployment size, deploys the appliance with 1905 GB of storage. • X-Large For tiny deployment size, deploys the appliance with 3245 GB of storage. For small deployment size, deploys the appliance with 3295 GB of storage. For medium deployment size, deploys the appliance with 3460 GB of storage. For large deployment size, deploys the appliance with 3525 GB of storage. For x-large deployment size, deploys the appliance with 3665 GB of storage.		
All deployment types	Name of the datastore on which you want to store the configuration files and virtual disks of the new appliance. **Note:** The installer displays a list of datastores that are accessible from your target server.	-	
	Enable or disable Thin Disk Mode.	Disabled	
All deployment types	Name of the network to which to connect the new appliance. **Note:** The installer displays a drop-down menu with networks that depend on the network settings of your target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu. The network must be accessible from the source server on which resides that appliance that you want to upgrade. The network must be accessible from the physical client machine from which you perform the deployment.	-	
	IP version for the appliance temporary address Can be either IPv4 or IPv6.	IPv4	
	IP assignment for the appliance temporary address Can be either static or DHCP.	static	
All deployment types Only if you use a static assignment for the temporary IP address.	Temporary system name (FQDN or IP address) The system name is used for managing the local system. The system name must be FQDN. If a DNS server is not available, provide a static IP address.	-	
	Temporary IP address	-	

Required for Upgrade of	Required Information	Default	Your Entry
	For IPv4 version, a subnet mask as a dot decimal notation or a network prefix as an integer between 0 and 32. For IPv6 version, a network prefix as an integer between 0 and 128.	-	
	Default gateway.	-	
	DNS servers separated by commas.	-	
All deployment types Only if you use a DHCP assignment with IPv4 version for the temporary IP address and a DDNS server is available in your environment.	Temporary system name (FQDN).	-	

Table 63: Required Information During Stage 2 of the Upgrade

Required for	Required Information	Default	Your Entry
• vCenter Server appliance 6.5 with an embedded or external Platform Services Controller • vCenter Server appliance 6.7 with an embedded or external Platform Services Controller	Data types to transfer from the old appliance to the new appliance. In addition to the configuration data, you can transfer the events, tasks, and, performance metrics. **Note:** For minimum upgrade time and storage requirement for the new appliance, select to transfer only the configuration data.	-	
• vCenter Server appliance 6.5 with an embedded Platform Services Controller • Platform Services Controller 6.5 appliance • vCenter Server appliance 6.7 with an embedded Platform Services Controller	Join or do not participate in the VMware Customer Experience Improvement Program (CEIP). For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.	Join the CEIP.	

Upgrade a vCenter Server Appliance 6.5 or 6.7 with an Embedded Platform Services Controller by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter Server appliance 6.5 or 6.7 that uses an embedded Platform Services Controller to vCenter Server appliance 7.0. You must run the GUI upgrade from a Windows, Linux, or Mac OS X machine that is in the same network as the appliance that you want to upgrade.

- See Prerequisites for Upgrading the vCenter Server Appliance.
- See Required Information for Upgrading a vCenter Server Appliance 6.5 or 6.7.

Stage 1 - Deploy the OVA File of the New vCenter Server Appliance

With stage 1 of the upgrade process, you deploy the OVA file, which is included in the vCenter Server appliance installer, for the new vCenter Server appliance.

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Upgrade**.
3. Review the Introduction page to understand the upgrade process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. Connect to the source appliance that you want to upgrade.
   a) Enter the information about the source vCenter Server appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the vCenter Server appliance that you want to upgrade.
Appliance HTTPS port	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with vCenter Server appliance version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

   b) Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important:** The user must be administrator@*your_domain_name*.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

   c) Enter the information about the source ESXi host or vCenter Server instance on which resides the vCenter Server appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the source ESXi host or vCenter Server instance on which the vCenter Server appliance that you want to upgrade resides. **Note:** The source vCenter Server instance cannot be the vCenter Server appliance that you want to upgrade. In such cases, use the source ESXi host.
HTTPS port	If the ESXi host or vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.

Option	Description
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

6. Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.
7. Connect to the target server on which you want to deploy the new vCenter Server appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the new appliance.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the new appliance. **Note:** The target server cannot be the vCenter Server appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

8. On the Set up target appliance VM page, enter a name for the new vCenter Server appliance, set the password for the root user, and click **Next**.

   The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

   The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

   Note: The root password of the old appliance is not transferred to the new upgraded appliance.
9. Select the deployment size for the new vCenter Server appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines

Deployment Size Option	Description
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

10. Select the storage size for the new vCenter Server appliance and click **Next**.

    Important: You must consider the storage size of the appliance that you are upgrading and the database size if external.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

11. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.

12. Configure the temporary network for communication between the vCenter Server appliance that you want to upgrade and the new vCenter Server appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important:** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.

Option	Action
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. • **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. • **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

13. On the Ready to complete stage 1 page, review the deployment settings for the new vCenter Server appliance and click **Finish** to start the OVA deployment process.
14. Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the new appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface of the newly deployed vCenter Server appliance to transfer the data from the old appliance and set up the services.

The newly deployed vCenter Server appliance 7.0 is running on the target server but is not configured.

Important: The data from the old appliance is not transferred and the services of the new appliance are not started.

Stage 2 - Transfer the Data and Set up the Newly Deployed vCenter Server Appliance With an Embedded Platform Services Controller

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server appliance 7.0.

Understand the data migration options available to you when upgrading or migrating to a vCenter Server appliance with an embedded PostgreSQL database. See Transferring Data After Upgrade or Migration.

1. Review the introduction to stage 2 of the upgrade process and click **Next**.
2. Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.
   - If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

     You cannot proceed with the upgrade until you have corrected the errors.

     Important: If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.
   - If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

     After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.

3. Connect to the source appliance that you want to upgrade.
   a) Enter the information about the source vCenter Server appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the vCenter Server appliance that you want to upgrade.
Appliance HTTPS port	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with vCenter Server appliance version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

   b) Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important:** The user must be administrator@*your_domain_name*.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

   c) Enter the information about the source ESXi host or vCenter Server instance on which resides the vCenter Server appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the source ESXi host or vCenter Server instance on which the vCenter Server appliance that you want to upgrade resides. **Note:** The source vCenter Server instance cannot be the vCenter Server appliance that you want to upgrade. In such cases, use the source ESXi host.
HTTPS port	If the ESXi host or vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

4. On the **Select migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server appliance.

5. Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

   For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

6. On the Ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.
7. Read the shutdown warning message and click **OK**.
8. Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

The vCenter Server appliance is upgraded. The old vCenter Server appliance is powered off and the new appliance starts.

- Verify Your vCenter Server Upgrade or Migration Is Successful.
- If the old vCenter Server appliance uses a non-ephemeral distributed virtual port group, to preserve the port group setting, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group. For information about configuring virtual machine networking on a vSphere distributed switch, see *vSphere Networking*.
- You can configure high availability for the vCenter Server appliance. For information about providing vCenter Server appliance high availability, see *vSphere Availability*.

Upgrade a vCenter Server Appliance 6.5 or 6.7 with an External Platform Services Controller Instance by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter Server appliance 6.5 or 6.7 that uses an external Platform Services Controller instance to vCenter Server appliance 7.0. You must run the GUI upgrade from a Windows, Linux, or Mac OS X computer that is in the same network as the appliance that you want to upgrade.

- The new vCenter Server appliance contains all Platform Services Controller services. It is no longer necessary nor possible to deploy and use an external Platform Services Controller, as all Platform Services Controller services are consolidated into vCenter Server. To learn more about this change to vCenter Server, see Removal of Platform Services Controller.
- See Prerequisites for Upgrading the vCenter Server Appliance.
- See Required Information for Upgrading a vCenter Server Appliance 6.5 or 6.7.

Stage 1 - Deploy the OVA File of the New vCenter Server Appliance 7.0

With stage 1 of the upgrade process, you deploy the OVA file of the new vCenter Server appliance 7.0.

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.

2. On the Home page, click **Upgrade**.
3. Review the Introduction page to understand the upgrade process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. Connect to the source appliance that you want to upgrade.
   a) Enter the information about the source vCenter Server appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the vCenter Server appliance that you want to upgrade.
Appliance HTTPS port	If the source appliance uses a custom HTTPS port, change the default value to that of the custom port. The default port value is 443. Custom port values are supported beginning with vCenter Server appliance version 6.5 Update 2. If you are upgrading from earlier versions, you cannot specify a custom port.

   b) Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important:** The user must be administrator@*your_domain_name*.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

   c) Enter the information about the source ESXi host or vCenter Server instance on which resides the vCenter Server appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the source ESXi host or vCenter Server instance on which the vCenter Server appliance that you want to upgrade resides. **Note:** The source vCenter Server instance cannot be the vCenter Server appliance that you want to upgrade. In such cases, use the source ESXi host.
HTTPS port	If the ESXi host or vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

6. Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.
7. Confirm that the vCenter Server appliance using an external Platform Services Controller will be converged to a vCenter Server appliance with the Platform Services Controller services consolidated within vCenter Server, and click **Yes** to accept and continue with the upgrade.
8. Connect to the target server on which you want to deploy the new vCenter Server appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the new appliance.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the new appliance. **Note:** The target server cannot be the vCenter Server appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

9. On the Set up target appliance VM page, enter a name for the new vCenter Server appliance, set the password for the root user, and click **Next**.

   The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

   The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

   Note: The root password of the old appliance is not transferred to the new upgraded appliance.

10. Select the deployment size for the new vCenter Server appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines

Deployment Size Option	Description
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

11. Select the storage size for the new vCenter Server appliance and click **Next**.

    Important: You must consider the storage size of the appliance that you are upgrading and the database size if external.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

12. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.
13. Configure the temporary network for communication between the vCenter Server appliance that you want to upgrade and the new vCenter Server appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important:** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.

Option	Action
Network type	Select the allocation method for the temporary IP address of the appliance. • **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. • **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

14. On the Ready to complete stage 1 page, review the deployment settings for the new vCenter Server appliance and click **Finish** to start the OVA deployment process.
15. Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the new appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface of the newly deployed vCenter Server appliance to transfer the data from the old appliance and set up the services.

The newly deployed target vCenter Server appliance 7.0 is running on the target server but is not configured.

Proceed to stage 2 of the upgrade process to transfer the data from the source vCenter Server appliance and start the services of the newly deployed vCenter Server appliance. See Stage 2 - Transfer the Data and Set up the Newly Deployed vCenter Server Appliance.

Stage 2 - Transfer the Data and Set up the Newly Deployed vCenter Server Appliance

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server appliance 7.0.

Understand the data migration options available to you when upgrading or migrating to a vCenter Server appliance with an embedded PostgreSQL database. See Transferring Data After Upgrade or Migration.

1. Review the introduction to stage 2 of the upgrade process and click **Next**.
2. Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.
   - If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

     You cannot proceed with the upgrade until you have corrected the errors.

     Important: If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.
   - If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

     After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.

3. Specify the replication topology for the vCenter Server. When converging vCenter Server instance with an external Platform Services Controller you must specify the replication topology.

   Convergence is the process of converting a vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with those services embedded in the appliance.

   - This is the first vCenter Server in the topology that I want to converge.
   - This is a subsequent vCenter Server.

     If this is a subsequent vCenter Server, provide the IP address of its partner vCenter Server and its HTTPS port.

4. On the **Select upgrade data** page, choose the types of data that you want to transfer from the old vCenter Server appliance to the new, upgraded vCenter Server appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data.

   Note: If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server appliance.

5. Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

   For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

6. On the Ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.
7. Read the shutdown warning message and click **OK**.
8. Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

The vCenter Server appliance is upgraded. The old vCenter Server appliance is powered off and the new appliance starts.

- Verify Your vCenter Server Upgrade or Migration Is Successful.
- If the old vCenter Server appliance uses a non-ephemeral distributed virtual port group, to preserve the port group setting, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group. For information about configuring virtual machine networking on a vSphere distributed switch, see *vSphere Networking*.
- Upgrade all vCenter Server instances in the vCenter Single Sign-On domain.
- After converging a vCenter Server with external Platform Services Controller to a vCenter Server appliance, you must decommission the original external Platform Services Controller. Decommissioning a Platform Services Controller shuts it down and removes it from the single sign-on domain. See Decommission the Platform Services Controller.
- You can configure high availability for the vCenter Server appliance. For information about providing vCenter Server appliance high availability, see *vSphere Availability*.

Upgrading vCenter Server in High Availability Environments

You can use the GUI installer to perform an interactive upgrade of a vCenter Server appliance in a high availability (HA) environment.

Prerequisites for Upgrading vCenter Server High Availability Environments

To ensure a successful upgrade of vCenter Server in a high availability (HA) environment, your environment must meet certain prerequisites before running the upgrade.

General Prerequisites

Ensure that your environment meets the prerequisites for upgrading vCenter Server appliance. See Prerequisites for Upgrading the vCenter Server Appliance.

High Availability Prerequisites

In addition to the prerequisites for upgrading a standard vCenter Server appliance, the vCenter High Availability (vCenter HA) upgrade has the following prerequisites.

- A vCenter HA cluster consists of three vCenter Server appliances that act as Active, Passive, and Witness nodes. The Active node must be configured as the vCenter HA node.
- The Active node is part of the vCenter HA cluster.
- All nodes must be present in the cluster.
- The vCenter HA cluster must be in a healthy state.
- The vCenter HA cluster must be in enabled mode.
- The host that has the vCenter Server virtual machine (VM) must be managed by a container vCenter Server. It must not be standalone.
- The target vCenter Server must have the same placement as the source vCenter Server.
- vCenter HA cannot be set up on a vCenter Server that has disks on more than one datastore.

To learn more about vCenter HA configuration, see *vSphere Availability*.

Upgrade a vCenter Server Appliance 6.5 or 6.7 HA Cluster with an Embedded Platform Services Controller by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter Server appliance 6.5 or 6.7 in a High Availability (HA) cluster that uses an embedded vCenter Single Sign-On or Platform Services Controller to vCenter Server appliance 7.0. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

- See Prerequisites for Upgrading vCenter Server High Availability Environments.
- See Required Information for Upgrading a vCenter Server Appliance 6.5 or 6.7.

You can deploy version 7.0 of the vCenter Server appliance on hosts that are running ESXi 6.5 or later and on vCenter Server instances 6.5 or later.

A vCenter HA cluster consists of three vCenter Server appliances that act as Active, Passive, and Witness nodes. The Active vCenter HA node is upgraded using a migration-based upgrade while preserving the existing configuration.

Stage 1 - Deploy the OVA File of the New vCenter High Availability Cluster

In stage 1 of the upgrade process, you deploy the OVA file for the new vCenter Server appliance.

Ensure that your environment meets the prerequisites for upgrading a vCenter HA cluster. See Prerequisites for Upgrading vCenter Server High Availability Environments.

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.

2. On the Home page, click **Upgrade**.
3. Review the Introduction page to understand the upgrade process and click **Next**.
4. Connect to the source appliance that you want to upgrade. This appliance is the Active vCenter HA node.
   a) Enter the information about the source vCenter Server appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the Active vCenter HA node that you want to upgrade.
Appliance HTTPS port	The default value (443) is displayed and cannot be edited.

   b) Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important:** The user must be administrator@*your_domain_name*.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

   c) Enter the information about the source vCenter Server instance on which resides the vCenter Server appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the Active node. The Active node must be configured as the vCenter HA node.
HTTPS port	If the vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

5. Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.
6. If vCenter HA is successfully detected, the target appliance is set to the manager of the source appliance. Click **OK**.

   The appliance deployment target information is populated.
7. On the Set up target appliance VM page, enter a name for the target vCenter Server appliance, set the password for the root user, and click **Next**.

   The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

   Note: The root password of the source is not transferred to the target appliance.
8. Select the deployment size for the new vCenter Server appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory.

Deployment Size Option	Description
	Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

9. Select the storage size for the new vCenter Server appliance and click **Next**.

   Important: You must consider the storage size of the appliance that you are upgrading and the database size if external.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

10. From the list of available datastores, select the location to store the virtual machine (VM) configuration files and virtual disks, and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.

    Note: vCenter HA cannot be set up on a vCenter Server that has disks on more than one datastore.

11. Configure the temporary network for communication between the vCenter Server appliance that you want to upgrade and the new vCenter Server appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily.

Option	Action
	The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important:** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. • **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. • **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

12. On the Ready to complete stage 1 page, review the deployment settings for the new vCenter Server appliance and click **Finish** to start the OVA deployment process.
13. Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the new appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface of the newly deployed vCenter Server appliance to transfer the data from the old appliance and set up the services.

The newly deployed vCenter Server appliance 7.0 is running on the target server but is not configured.

Important: The data from the old appliance is not transferred and the services of the new appliance are not started.

Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server appliance. When the deployment finishes, vCenter Server has high availability protection.

Understand the data migration options available to you when upgrading or migrating to a vCenter Server appliance with an embedded PostgreSQL database. You can select to migrate historical and other types of data in the background after deploying and starting vCenter Server. See Transferring Data After Upgrade or Migration.

1. Review the introduction to stage 2 of the deployment process and click **Next**.
2. Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.
   - If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

     You cannot proceed with the upgrade until you have corrected the errors.

     Important: If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.
   - If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

     After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.
3. On the **Select migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server appliance.
4. Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

   For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.
5. On the Ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.
6. Read the shutdown warning message and click **OK**.
7. Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

The vCenter Server appliance is upgraded. The old vCenter Server appliance is powered off and the new appliance starts.

After the Active node is upgraded, Auto Deployment automatically creates new Passive and Witness nodes using a clone operation. For Manual Deployment, nodes are not created automatically. You must clone the Passive and Witness virtual machines, and set the cluster mode to **Enabled**.

When the deployment finishes, vCenter Server has high availability protection. You can click **Edit** to enter Maintenance Mode, Deactivate, or Remove vCenter HA. You can also Initiate vCenter HA failover.

For information about configuring and managing vCenter HA, see *vSphere Availability*.

Upgrade a vCenter 6.5 or 6.7 HA Cluster with an External Platform Services Controller by Using the GUI

You can use the GUI installer to perform an interactive upgrade of a vCenter HA cluster 6.5 or 6.7 that uses an external Platform Services Controller instance to vCenter Server appliance 7.0. You must run the GUI upgrade from a Windows, Linux, or Macintosh computer that is in the same network as the appliance that you want to upgrade.

- The new vCenter Server appliance contains all Platform Services Controller services. It is no longer necessary nor possible to deploy and use an external Platform Services Controller, as all Platform Services Controller services

are consolidated into vCenter Server. To learn more about this change to vCenter Server, see Removal of Platform Services Controller.

- Ensure that your environment meets the prerequisites for upgrading a vCenter HA cluster. See Prerequisites for Upgrading vCenter Server High Availability Environments.
- See Required Information for Upgrading a vCenter Server Appliance 6.5 or 6.7.

A vCenter HA cluster consists of three vCenter Server appliances that act as Active, Passive, and Witness nodes. The Active vCenter HA node is upgraded using a migration-based upgrade while preserving the existing configuration.

Stage 1 - Deploy the OVA File of the New vCenter High Availability Cluster

With stage 1 of the upgrade process, you deploy the OVA file of the new vCenter Server appliance 7.0.

Ensure that your environment meets the prerequisites for upgrading a vCenter HA cluster. See Prerequisites for Upgrading vCenter Server High Availability Environments.

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Upgrade**.
3. Review the Introduction page to understand the upgrade process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. Connect to the source appliance that you want to upgrade. This appliance is the Active vCenter HA node.
   a) Enter the information about the source vCenter Server appliance that you want to upgrade, and click **Connect to Source**.

Option	Action
Appliance FQDN or IP address	Enter the IP address or FQDN of the Active vCenter HA node that you want to upgrade.
Appliance HTTPS port	The default value (443) is displayed and cannot be edited.

   b) Enter the information about the vCenter Single Sign-On administrator and root user.

Option	Action
SSO user name	Enter the vCenter Single Sign-On administrator user name. **Important:** The user must be administrator@*your_domain_name*.
SSO password	Enter the password of the vCenter Single Sign-On administrator.
Appliance (OS) root password	Enter the password of the root user.

   c) Enter the information about the source vCenter Server instance on which resides the vCenter Server appliance that you want to upgrade and click **Next**.

Option	Description
Source server or host name	IP address or FQDN of the Active node. The Active node must be configured as the vCenter HA node.

Option	Description
HTTPS port	If the vCenter Server instance uses a custom HTTPS port, change the default value. The default value is 443.
User name	User name of a user with administrative privileges on the ESXi host or vCenter Server instance.
Password	Password of the user with administrative privileges on the ESXi host or vCenter Server instance.

6. Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and its source server, and click **Yes** to accept the certificate thumbprints.
7. Confirm that the vCenter Server appliance using an external Platform Services Controller will be converged to a vCenter Server appliance with the Platform Services Controller services consolidated within vCenter Server, and click **Yes** to accept and continue with the upgrade.
8. If vCenter Server HA is successfully detected, the target appliance is set to the manager of the source appliance. Click OK.

   The appliance deployment target information is populated.
9. Connect to the target server on which you want to deploy the new vCenter Server appliance.

Option	Steps
You can connect to an ESXi host on which to deploy the new appliance.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the new appliance. **Note:** The target server cannot be the vCenter Server appliance that you want to upgrade. In such cases, use an ESXi host as a target server.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

10. On the Set up target appliance VM page, enter a name for the new vCenter Server appliance, set the password for the root user, and click **Next**.

    The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.

    The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

    Note: The root password of the old appliance is not transferred to the new upgraded appliance.

11. Select the deployment size for the new vCenter Server appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

12. Select the storage size for the new vCenter Server appliance, and click **Next**.

    Important: You must consider the storage size of the appliance that you are upgrading and the database size if external.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

13. From the list of available datastores, select the location to store the virtual machine (VM) configuration files and virtual disks, and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.

    Note: vCenter HA cannot be set up on a vCenter Server that has disks on more than one datastore.

14. Configure the temporary network for communication between the vCenter Server appliance that you want to upgrade and the new vCenter Server appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important:** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. • **Static** The wizard prompts you to enter the temporary IP address, subnet mask or prefix length, default gateway, and DNS servers. • **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment. Optionally, you can provide a temporary system name (FQDN) if a DDNS server is available in your environment.

15. On the Ready to complete stage 1 page, review the deployment settings for the new vCenter Server appliance and click **Finish** to start the OVA deployment process.

16. Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the new appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface of the newly deployed vCenter Server appliance to transfer the data from the old appliance and set up the services.

The newly deployed target vCenter Server appliance 7.0 is running on the target server but is not configured.

Important: The data from the source vCenter Server is not transferred and the services of the target appliance are not started.

Transfer the data from the old appliance and start the services of the newly deployed vCenter Server Appliance. See Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster.

Stage 2 - Transfer Data and Set-Up the Newly Deployed vCenter High Availability Cluster

When the OVA deployment finishes, you are redirected to stage 2 of the upgrade process to transfer the data from the old appliance and start the services of the newly deployed vCenter Server appliance. When the deployment finishes, vCenter Server has high availability protection.

Understand the data migration options available to you when upgrading or migrating to a vCenter Server appliance with an embedded PostgreSQL database. You can select to migrate historical and other types of data in the background after deploying and starting vCenter Server. See Transferring Data After Upgrade or Migration.

1. Review the introduction to stage 2 of the upgrade process and click **Next**.
2. Wait for the pre-upgrade check to finish and read the pre-upgrade check result if any.
   - If the pre-upgrade check result contains error messages, read the messages and click **Logs** to export and download a support bundle for troubleshooting.

     You cannot proceed with the upgrade until you have corrected the errors.

     Important: If you have provided incorrect vCenter Single Sign-On user name and password of the source appliance during stage 1, the pre-upgrade check fails with an authentication error.
   - If the pre-upgrade check result contains warning messages, read the messages and click **Close**.

     After you have verified that your system meets the requirements from the warning message, you can proceed with the upgrade.
3. Specify the replication topology for the vCenter Server. When converging vCenter Server instance with an external Platform Services Controller you must specify the replication topology.

   Convergence is the process of converting a vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with those services embedded in the appliance.
   - This is the first vCenter Server in the topology that I want to converge.
   - This is a subsequent vCenter Server.

     If this is a subsequent vCenter Server, provide the IP address of its partner vCenter Server and its HTTPS port.
4. On the **Select migration data** page, choose the types of data that you want to transfer from the old appliance to the new, upgraded appliance.

   A large amount of data requires more time to be transferred to the new appliance. For the minimum upgrade time and storage requirements for the new appliance, select to transfer only the configuration data. If you are using an external Oracle database, you can also choose to migrate historical and performance metrics data in the background after you deploy and start the new vCenter Server appliance.
5. On the Ready to complete page, review the upgrade settings, accept the backup acknowledgment, and click **Finish**.
6. Read the shutdown warning message and click **OK**.
7. Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

The vCenter Server appliance is upgraded. The old vCenter Server appliance is powered off and the new appliance starts.

After the Active node is upgraded, a new Passive and Witness node is created using a clone operation. These nodes are created automatically for Auto Deployment. For Manual Deployment, nodes are not created automatically. You must clone the Passive and Witness VMs and set the cluster mode to **enabled**.

When the deployment finishes, vCenter Server has high availability protection. You can click **Edit** to enter Maintenance Mode, Deactivate, or Remove vCenter HA. You can also Initiate vCenter HA failover.

- Verify Your vCenter Server Upgrade or Migration Is Successful.

- If the old vCenter Server appliance uses a non-ephemeral distributed virtual port group, to preserve the port group setting, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group. For information about configuring virtual machine networking on a vSphere distributed switch, see *vSphere Networking*.
- Upgrade all vCenter Server instances in the vCenter Single Sign-On domain.
- After converging a vCenter Server with external Platform Services Controller node to vCenter Server Appliance, you must decommission the original external Platform Services Controller. Decommissioning a Platform Services Controller shuts it down and removes it from the single sign-on domain. See Decommission the Platform Services Controller.
- You can configure high availability for the vCenter Server appliance. For information about providing vCenter Server appliance high availability, see *vSphere Availability*.

CLI Upgrade of the vCenter Server Appliance

You can use the CLI installer to perform an unattended upgrade of a vCenter Server appliance on an ESXi host or vCenter Server instance.

The CLI upgrade process includes downloading the vCenter Server appliance installer on a network virtual machine or physical server from which you want to perform the upgrade, preparing a JSON configuration file with the upgrade information, and running the upgrade command.

Important: The user name that you use to log in to the machine from which you want to run the CLI upgrade, the path to the vCenter Server appliance ISO file, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

The vCenter Server appliance ISO file contains templates of JSON files that contain the minimum configuration parameters that are required for upgrading a vCenter Server appliance. For information about preparing JSON templates for CLI upgrade of the vCenter Server appliance, see Prepare Your JSON Configuration File for CLI Upgrade.

Note:

Note: When you upgrade vCenter Server 6.5 or 6.7 with an external Platform Services Controller to vCenter Server7.0, the upgrade process converges the external Platform Services Controller into the new vCenter Server appliance. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to upgrade and use an external Platform Services Controller.

After successfully upgrading your environment to vCenter Server7.0, the pre-existing Platform Services Controller will be powered off, and you can remove it from your vSphere inventory. See Decommission the Platform Services Controller.

Prepare Your JSON Configuration File for CLI Upgrade

Before you run the CLI command to upgrade a vCenter Server appliance, you must prepare a JSON file with configuration parameters and their values for your upgrade specification.

- You must be familiar with the JSON syntax.
- Download and Mount the vCenter Server Installer.

The vCenter Server installer contains JSON templates for all upgrade types. For information about the templates, see JSON Templates for CLI Upgrade of the vCenter Server Appliance.

You can upgrade an appliance with minimum configurations by setting values to the configuration parameters in the JSON template for your specification. You can edit the preset values, remove configuration parameters, and add configuration parameters for custom configurations.

For a complete list of the configuration parameters and their descriptions, navigate to the installer subdirectory for your operating system and run the `vcsa-deploy upgrade --template-help` command or see Upgrade Configuration Parameters for CLI Upgrade of vCenter Server Appliance .

1. In the vCenter Server Appliance installer, navigate to the `vcsa-cli-installer` directory, and open the `templates` subfolder.
2. Copy the upgrade templates from the `upgrade` subfolder to your workspace.

   Important: The path to the JSON configuration files must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.
3. Open the template file for your use case in a text editor.

   To ensure the correct syntax of your JSON configuration file, use a JSON editor.
4. Fill in the values for the required configuration parameters and, optionally, enter additional parameters and their values.
   For example, if you want to use an IPv4 DHCP assignment for the temporary network of the new appliance, in the `temporary_network` subsection of the template, change the value of the `mode` parameter to `dhcp` and remove the default configuration parameters that are for a static assignment.

   ```
   "temporary_network": {
       "ip_family": "ipv4",
       "mode": "dhcp"
   },
   ```

   Important: The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

   To set a value that contains a backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-6.7.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-6.7.0.XXXX-YYYYYYY_OVF10.ova`.

   The Boolean values must contain only lowercase characters, that is, a value can be either `true` or `false` . For example, `"ssh_enable":false` .
5. Optional: Use a JSON editor of your choice to validate the JSON file.
6. Save in UTF-8 format and close the file.

You can create and save additional templates if needed for your upgrade specification.

JSON Templates for CLI Upgrade of the vCenter Server Appliance

The vCenter Server appliance installer contains JSON templates that are located in the `vcsa-cli-installer/templates` directory. In the `upgrade` subfolder, you can find the JSON templates with the minimum configuration parameters for all upgrade types.

For each upgrade type, there is one template for deploying the new appliance on an ESXi host and another template for deploying the new appliance on a vCenter Server instance.

Table 64: Upgrade JSON Templates Included in the vCenter Server Appliance Installer

Location	Template	Description
vcsa-cli-installer\templates\upgrade\vcsa\6.5	embedded_vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.5 with an embedded Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.
	embedded_vCSA_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.5 with an embedded Platform Services ControllervCenter Server appliance 7.0 on a vCenter Server instance.
	vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.5 with an external Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.
	vCSA_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.5 with an external Platform Services Controller to vCenter Server appliance 7.0 on a vCenter Server instance.
vcsa-cli-installer\templates\upgrade\vcsa\6.7	embedded_vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.7 with an embedded Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.
	embedded_vCSA_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.7 with an embedded Platform Services Controller to vCenter Server Appliance7.0 on a vCenter Server instance.
	vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.7 with an external Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.

Location	Template	Description
	vCSA_on_VC.json	Contains the minimum configuration parameters that are required for upgrade of a vCenter Server appliance 6.7 with an external Platform Services Controller to vCenter Server appliance 7.0 on a vCenter Server instance.

About Upgrading a vCenter Server with an External Platform Services Controller Using the CLI

When upgrading a vCenter Server appliance that uses an external Platform Services Controller, it is converted to a vCenter Server instance with those services embedded in the appliance. For this reason, you must specify replication partner parameters in the JSON upgrade templates.

When upgrading a vCenter Server appliance that uses an external Platform Services Controller, you must specify replication partner parameters in the JSON upgrade template. These parameters indicate if the upgrade is for one of the following vCenter Server and Platform Services Controller upgrade scenarios.

- A single vCenter Server and a single Platform Services Controller instance within an SSO domain.
- The first vCenter Server and Platform Services Controller instance within an SSO domain containing more than one vCenter Server.
- Replicating vCenter Server and Platform Services Controller instances within an SSO domain, which you must point to an existing vCenter Server 7.0 instance as the replication partner.

Important: It is not possible to upgrade an external Platform Services Controller. The upgrade process converges the Platform Services Controller services into the vCenter Server appliance. For more information, see Removal of Platform Services Controller.

Deployments using an external Platform Services Controller are often called an MxNdeployment, where M represents the vCenter Server, and N represents the external Platform Services Controller. When representing multiple instances of vCenter Server and Platform Services Controller in a domain, this is expressed as M*n*xN*n*, where *n* is the number of instances. For example, M2xN2 indicates two vCenter Server instances and two Platform Services Controller instances within the same domain. When upgrading such a deployment, you first upgrade one instance to version 7.0, and then upgrade the second instance to 7.0, specifying the first of the two instances as the replicating partner.

The replication parameters in the JSON upgrade template are located in the sso section of the template, and are first_instance and replication_partner_hostname .

Parameter Name	Description
first_instance	The first_instance parameter identifies the vCenter Server as either the first instance in your vCenter Server SSO domain, or as a replicating partner. If it is the first vCenter Server instance, set first_instance to true For additional instances of vCenter Server in the same SSO domain, set first_instance to false .
replication_partner_hostname *	If you set first_instance to false , you must specify the FQDN or IP address of a vCenter Server that has already been upgraded to version 7.0, and whose external PSC has been converged into the vCenter Server appliance.

When you perform the CLI upgrade of a single vCenter Server appliance that uses an external Platform Services Controller, the process is as follows:

1. Upgrade the vCenter Server instance in your topology using the `vCSA_on_ESXi.json` template when upgrading on ESXi, or the `vCSA_on_VC.json` template when upgrading on a vCenter Server deployment.
2. For a deployment topology consisting of a single vCenter Server and a Platform Services Controller (an `M1xN1` deployment), edit the `sso` section of the template such that the `first_instance` parameter is set to `true` , and remove the `replication_partner_hostname` parameter.

```
"sso": {
"__comments": [ This is the first instance (M1) vCenter Server management node, with "first_instance" set
 to "true" and "replication_partner_hostname" removed.
],
"first_instance": true
}
```

3. Specify the remaining upgrade configuration parameters in the JSON template, and upgrade vCenter Server to version 7.0 using the CLI. See Upgrade a vCenter Server Appliance by Using the CLI.
4. After successfully upgrading vCenter Server, decommission the Platform Services Controller. See Decommission the Platform Services Controller.

   Important: Decommission the Platform Services Controller instances only after upgrading and converging all vCenter Server instances in your topology.

For a deployment consisting of two or more vCenter Server and Platform Services Controller instances (an `M2xN2` deployment), you first upgrade the `M1`vCenter Server instance to version 7.0, and then upgrade the second, replicating vCenter Server instance.

1. Upgrade the vCenter Server instances in your deployment using the `vCSA_on_ESXi.json` template when upgrading on ESXi, or the `vCSA_on_VC.json` template when upgrading on a vCenter Server deployment.
2. For the first vCenter Server instance (`M1`), edit the `sso` section of the template such that the `first_instance` parameter is set to `true` , and remove the `replication_partner_hostname` parameter.

```
"sso": {
"__comments": [ This is the first instance (M1) vCenter Server management node, with "first_instance" set
 to "true" and "replication_partner_hostname" removed.
],
"first_instance": true
}
```

3. For the remaining vCenter Server instance (`M2`), edit the `sso` section of the template such that the `first_instance` parameter is set to `false` , and provide the FQDN or IP address of the vCenter Server instance to which you want to replicate the second node. The replication partner is the first vCenter Server instance (`M1`) you upgraded to version 7.0, which has been converged with its Platform Services Controller instance.

```
"sso": {
"__comments": [ This is the second instance (M2) vCenter Server management node, with "first_instance" set
 to "false" and "replication_partner_hostname" set to the hostname of the replication partner.],
"first_instance": false,
"replication_partner_hostname": "FQDN_or_IP_address"
```

4. Specify the remaining upgrade configuration parameters in the JSON templates, and finish the upgrade using the CLI. See Upgrade a vCenter Server Appliance by Using the CLI.
5. After successfully upgrading all vCenter Server instances in the topology, decommission the Platform Services Controller instances. See Decommission the Platform Services Controller.

   Important: Decommission the Platform Services Controller instances only after upgrading and converging all vCenter Server instances in your topology.

Upgrade Configuration Parameters for CLI Upgrade of vCenter Server Appliance

When you prepare your JSON configuration files for CLI upgrade, you must set parameters and values to provide input data for the upgrade of a vCenter Server appliance.

Sections and Subsections of Configuration Parameters in the JSON Upgrade Files

The configuration parameters in the JSON configuration files for CLI upgrade are organized in sections and subsections.

Table 65: Sections and Subsections of Configuration Parameters in the JSON Upgrade Files

Section	Subsection	Description
`new_vcsa` - describes the new appliance that you want to deploy.	`esxi`	Use only if you want to deploy the new appliance directly on an ESXi host. Contains the configuration parameters that describe the target ESXi host. See Table 66: Configuration Parameters in the new_vcsa Section, esxi Subsection. **Note:** You must fill in either this subsection or the `vc` subsection.
	`vc`	Use only if you want to deploy the new appliance on the inventory of a vCenter Server instance. Contains the configuration parameters that describe the target ESXi host or DRS cluster from the vCenter Server inventory. See Table 67: Configuration Parameters in the new_vcsa Section, vc Subsection. **Note:** You must fill in either this subsection or the `esxi` subsection. The target vCenter Server instance cannot be the vCenter Server Appliance that you want to upgrade. In such cases, use the `esxi` subsection.
	`appliance`	Contains the configuration parameters that describe the new appliance. See Table 68: Configuration Parameters in the new_vcsa Section, appliance Subsection
	`os`	Contains only the `ssh_enable` configuration parameter to set the SSH administrator login to the new appliance.
	`ovftool_arguments`	Optional. Use this subsection for adding arbitrary arguments and their values to the OVF Tool command that the installer generates. **Important:** The vCenter Server appliance installer does not validate the configuration parameters in the `ovftool_arguments` subsection. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
	`temporary_network`	Contains the configuration parameters that describe the temporary network settings for the new appliance. See Table 69: Configuration Parameters in the new_vcsa Section, temporary_network Subsection
	`user_options`	Contains only the `vcdb_migrateSet` configuration parameter to set the types of data that you want to transfer from the old appliance to the new appliance. See Table 70: Configuration Parameters in the new_vcsa Section, user_options Subsection
`source_vc` - describes the existing appliance that you want to upgrade.	`managing_esxi_or_vc`	Contains the configuration parameters that describe the source ESXi host or vCenter Server appliance instance on which resides the appliance that you want to upgrade. See Table 72: Configuration Parameters in the source_vc Section, managing_esxi_or_vc Subsection.
	`vc_vcsa`	Contains the configuration parameters that describe the source appliance that you want to upgrade. See Table 73: Configuration Parameters in the source_vc Section, vc_vcsa Subsection.

Section	Subsection	Description
`source_vum` - describes the source VMware Update Manager instance. Use if you want to automatically run Migration Assistant on the VMware Update Manager instance.	`run_migration_assistant`	Optional if the source vCenter Server appliance that you want to upgrade is connected to a VMware Update Manager instance that runs on a Windows virtual machine. Use this subsection if you want to automatically run Migration Assistant on the source VMware Update Manager instance. Contains the configuration parameters that describe the source VMware Update Manager instance, which will be migrated to the new upgraded vCenter Server appliance. See Table 74: Configuration Parameters in the source_vum Section, run_migration_assistant Subsection. **Note:** The Migration Assistant uses port 9123 by default. If port 9123 is used by another service on the Update Manager machine, Migration Assistant automatically finds another free port. You cannot set a custom port for Migration Assistant.
`ceip` - describes joining the VMware Customer Experience Improvement Program (CEIP).	`settings`	Contains only the `ceip_enabled` configuration parameter to join or not to join the VMware Customer Experience Improvement Program (CEIP). See Table 75: Configuration Parameters in the ceip Section, settings Subsection. Required only if you are upgrading a vCenter Server appliance with an embedded Platform Services Controller or a Platform Services Controller appliance. **Note:** If the `ceip_enabled` configuration parameter is set to `true` , you must run the CLI deployment command with the `--acknowledge-ceip` argument. For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

Important: The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To set a value that contains a backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"G:\\vcsa\\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYYY_OVF10.ova"` sets the path `G:\vcsa\VMware-vCenter-Server-Appliance-7.0.0.XXXX-YYYYYYY_OVF10.ova`.

The Boolean values must contain only lowercase characters. Can be either `true` or `false` . For example, `"ssh_enable":false` .

Configuration Parameters in the `new_vcsa` Section

Table 66: Configuration Parameters in the `new_vcsa` Section, `esxi` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target ESXi host on which you want to deploy the new appliance.
`username`	string	A user name with administrative privileges on the target ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the target ESXi host.
`deployment_network`	string	The name of the network to which to connect the new appliance. The network must be part of the target ESXi host or vCenter Server appliance instance (as identified by the `managing_esxi_or_vc` configuration parameter) network configuration. **Note:** The network must be accessible from the source ESXi host or vCenter Server appliance instance (as identified by the `managing_esxi_or_vc` configuration parameter) on which resides the appliance that you want to upgrade. The network must be also accessible from the client machine from which you are performing the upgrade. Ignored if the target ESXi host has only one network.

Name	Type	Description
datastore	string	The name of the datastore on which to store the virtual machine configuration files and virtual disks of the new appliance. The datastore must be available to the target ESXi host. **Note:** The datastore must have at least 25 GB of free space.
port	integer	The HTTPS reverse proxy port of the target ESXi host. The default port is 443. Use only if the target ESXi host uses a custom HTTPS reverse proxy port.

ssl_certificate_verification	string	The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI stops the upgrade unless you specify one of the following SSL certificate configuration options:
		Specify the Secure Hash Algorithm 1 (SHA-1) certificate thumbprint. A certificate thumbprint is a hexadecimal string that uniquely identifies a certificate. The thumbprint is calculated from the content of the certificate using a thumbprint algorithm.
		`"thumbprint": "certificate SHA-1 thumbprint"`
		Set verification_mode to NONE .
		`"verification_mode": "NONE"`
		If you are connecting to a server with a self-signed certificate, and fail to either specify the SHA-1 certificate thumbprint or set the verification mode to NONE , the CLI displays the server's self-signed certificate thumbprint, and prompts you to accept or reject the certificate thumbprint.
		You may also specify that the CLI ignore the self-signed using the vcsa-deploy upgrade command parameter --no-ssl-certificate-validation . See Syntax of the CLI Upgrade Command .

Table 67: Configuration Parameters in the new_vcsa Section, vc Subsection

Name	Type	Description
hostname	string	The IP address or FQDN of the target vCenter Server instance on which you want to deploy the new appliance.
username	string	vCenter Single Sign-On administrator user name on the target vCenter Server instance, for example, administrator@vsphere.local.
password	string	The password of the vCenter Single Sign-On administrator user on the target vCenter Server instance.
deployment_network	string	The name of the network to which to connect the new appliance. The network must part of the target ESXi host or DRS cluster network configuration. **Note:** The network must be accessible from the source ESXi host on which resides the appliance that you want to upgrade. The network must be also accessible from the client machine from which you are performing the upgrade. Ignored if the target ESXi host or DRS cluster has only one network.

datacenter	array	The vCenter Server data center that contains the target ESXi host or DRS cluster on which you want to deploy the new appliance.
		If the data center is located in a folder or a structure of folders, specify the as a comma-separated list of strings. For example,
		`["parent_folder", "child_folder", "datacenter_name"]`
		If there is no folder path on the data center, then use only the data center name. For example,
		`["datacenter_name"]`
		or
		`"datacenter_name"`

Name	Type	Description
		Note: The value is case-sensitive.
`datastore`	string	The name of the datastore that you want to store all virtual machine configuration files and virtual disks of the new appliance. **Note:** The datastore must be available to the target ESXi host or DRS cluster. The datastore must have at least 25 GB of free space.
`port`	integer	The HTTPS reverse proxy port of the target vCenter Server instance. The default port is 443. Use only if the target vCenter Server instance uses a custom HTTPS reverse proxy port.

`target`	array	The target cluster, ESXi host, or resource pool on which you want to deploy the new appliance. This is the target you specified with the `datacenter` parameter. This path must end with a cluster name, ESXi hostname, or resource pool name.
		Important: You must provide the name that is displayed in the vCenter Server inventory. For example, if the name of the target ESXi host is an IP address in the vCenter Server inventory, you cannot provide an FQDN.
		Note: All values are case-sensitive.
		If you want the deployed appliance to be listed in a different location within the data center's hierarchy, use the `vm_folder` parameter described later in this section.
		If the target cluster, ESXi host, or resource pool is located in a folder or a structure of folders, specify the value as a comma-separated list of strings. For example,
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		If the target ESXi host is part of a cluster, specify the path as a comma-separated list of strings. For example,
		`["cluster_name","esxi-host.domain.com"]`
		If you are deploying to a resource pool, include the label `Resources` before the resource pool name. For example:
		`["cluster_name", "Resources", "resource_pool_name"]`
		Note: Pre-checks verify only the memory of the resource pool.

`vm_folder`	string	Optional. The name of the virtual machine (VM) folder to which to add the new appliance.

Table 68: Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection

Name	Type	Description
`thin_disk_mode`	Boolean	Set to `true` to deploy the new appliance with thin virtual disks.
`deployment_option`	string	The size for the new appliance. **Note:** You must consider the database size of the appliance that you want to upgrade. For an external database, see Determine the Oracle Database Size and the Storage Size for the New Appliance. • Set to `tiny` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 300 GB of storage. • Set to `tiny-lstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 825 GB of storage. • Set to `tiny-xlstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 1700 GB of storage.

Name	Type	Description
		• Set to `small` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 340 GB of storage. • Set to `small-lstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 870 GB of storage. • Set to `small-xlstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 1750 GB of storage. • Set to `medium` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 525 GB of storage. • Set to `medium-lstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1025 GB of storage. • Set to `medium-xlstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1905 GB of storage. • Set to `large` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 740 GB of storage. • Set to `large-lstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1090 GB of storage. • Set to `large-xlstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1970 GB of storage. • Set to `xlarge` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1180 GB of storage. • Set to `xlarge-lstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1230 GB of storage. • Set to `xlarge-xlstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 2110 GB of storage. • Set to `management-tiny` if you want to deploy a vCenter Server appliance with an external Platform Services Controller for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 300 GB of storage.
`image`	string	Optional. A local file path or URL to the vCenter Server appliance installation package. By default the installer uses the installation package that is included in the ISO file, in the `vcsa` folder.
`name`	string	The VM name for the new appliance. Must contain only ASCII characters except a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
`ovftool_path`	string	Optional. A local file path to the OVF Tool executable file. By default the installer uses the OVF Tool instance that is included in the ISO file, in the `vcsa/ovftool` folder.

Table 69: Configuration Parameters in the `new_vcsa` Section, `temporary_network` Subsection

Name	Type	Description
`ip_family`	string	IP version for the temporary network of the new appliance. Set to `ipv4` or `ipv6` .
`mode`	string	IP assignment for the temporary network of the new appliance. Set to `static` or `dhcp` .
`ip`	string	Temporary IP address for the new appliance. Required only if you use a static assignment, that is, if you set the `mode` parameter to `static` . You must set an IPv4 or IPv6 address that corresponds to the temporary network IP version, that is, to the value of the `ip.family` parameter. An IPv4 address must comply with the RFC 790 guidelines. An IPv6 address must comply with the RFC 2373 guidelines.

`dns_servers`	string or array	IP addresses of one or more DNS servers for the temporary network of the new appliance.
		To set more than one DNS server, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["x.y.z.a", "x.y.z.b"]`
		or
		`"x.y.z.a, x.y.z.b"`
		Required only if you use static network mode for the temporary IP address allocation, that is, if you set the `mode` parameter to `static` .

`prefix`	string	Network prefix length for the temporary network of the new appliance. Use only if the `mode` parameter is set to `static` . Remove if the `mode` parameter is set to `dhcp` . The network prefix length is the number of bits that are set in the subnet mask. For example, if the subnet mask is 255.255.255.0, there are 24 bits in the binary version of the prefix length, so the network prefix length is 24. For IPv4 version, the value must be between `0` and `32` . For IPv6 version, the value must be between `0` and `128` .
`gateway`	string	IP address of the default gateway for the temporary network of the new appliance. For IPv6 version, the value can be `default` .

Table 70: Configuration Parameters in the `new_vcsa` Section, `user_options` Subsection

Name	Type	Description
`vcdb_migrateSet`	string	Select the types of data to migrate from the old appliance to the new appliance. Data is copied from the source vCenter Server to the target server. The original source of the data remains unchanged. • Set to `core` if you want to transfer only the configuration data. This option provides the fastest data migration, keeping system downtime to a minimum. • Set to `core_events_tasks` if you want to transfer the configuration and historical data (events and tasks) immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server appliance. • Set to `all` if you want to transfer the configuration, historical, and performance metrics data immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Windows. This option transfers the largest amount of data, and requires more downtime than other data migration options.

Name	Type	Description
		• Set to `transfer_events_tasks_after_upgrade` if you want to transfer the historical data (events and tasks) in the background after the upgrade finishes. During this time, vCenter Server performance might not be optimal. • Set to `transfer_stats_events_tasks_after_upgrade` if you want to transfer historical data and performance metrics data in the background after the upgrade finishes. During this time, vCenter Server performance might not be optimal. **Note:** To minimize the upgrade time and the amount of storage required for the new vCenter Server appliance, use the `core` value. For more information on the types of data you can transfer from your existing vCenter Server to the new, upgraded vCenter Server, see Transferring Data After Upgrade or Migration.

Table 71: Configuration Parameters in the `new_vcsa` Section, `sso` Subsection

Name	Type	Description
`first_instance`	string	Set `first_instance` to `true` if this is the first converge upgrade operation in your vCenter Server SSO domain, or if you do not want to set the replication partner for this node. If you want to set the replication partner for this node, set `first_instance` to `false` and provide the value of the `replication_partner_hostname` as the FQDN of a previously converged node which is currently in an embedded vCenter Server topology. For more information on specifying the `first_instance` and `replication_partner_hostname` parameters, see About Upgrading a vCenter Server with an External Platform Services Controller Using the CLI.
`replication_partner_hostname`	string	Host name of the replication partner. Remove if it is the `first_instance`.

Configuration Parameters in the `source_vc` Section

Table 72: Configuration Parameters in the `source_vc` Section, `managing_esxi_or_vc` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the source ESXi or vCenter Server host on which resides the appliance that you want to upgrade.
`username`	string	A user name with administrative privileges on the source ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the source ESXi host.
`port`	integer	The HTTPS reverse proxy port of the source ESXi host. The default port is 443. Use only if the source ESXi host uses a custom HTTPS reverse proxy port.

Table 73: Configuration Parameters in the `source_vc` Section, `vc_vcsa` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the source appliance that you want to upgrade.
`username`	string	vCenter Single Sign-On administrator user on the source appliance, for example administrator@vsphere.local. **Important:** The user must be administrator@*`your_domain_name`*.

Name	Type	Description
password	string	The password of the vCenter Single Sign-On administrator user on the source appliance.
root_password	string	The password for the root user of the operating system of the source appliance.
export_dir	string	Directory to export source configuration and data.

Configuration Parameters in the `source.vum` Section

Table 74: Configuration Parameters in the `source_vum` Section, `run_migration_assistant` Subsection

Name	Type	Description
esxi_hostname	string	The IP address or FQDN of the ESXi host on which resides the source VMware Update Manager instance. If an FQDN is provided, it must be resolvable from the client machine from which you run the upgrade.
esxi_username	string	A user name with administrative privileges on the ESXi host, for example, root.
esxi_password	string	The password of the user with administrative privileges on the ESXi host.
esxi_port	string	The HTTPS reverse proxy port of the ESXi host. The default port is 443. Use only if the ESXi host uses a custom HTTPS reverse proxy port.
vum_hostname	string	The IP address or FQDN of the Windows virtual machine on which the source VMware Update Manager instance runs. If an FQDN is provided, it must be resolvable from the client machine from which you run the upgrade.
vum_os_username	string	The administrator user name of the Windows virtual machine on which the source VMware Update Manager instance runs.
vum_os_password	string	The administrator password of the Windows virtual machine on which the source VMware Update Manager instance runs. If not provided, you are prompted to enter the password at the command console during the template verification.
export_dir	string	Directory to export source configuration and data.

Configuration Parameters in the `ceip` Section

Table 75: Configuration Parameters in the `ceip` Section, `settings` Subsection

Name	Type	Description
ceip_enabled	Boolean	Set to `true` to join the CEIP for the new upgraded appliance.

Upgrade a vCenter Server Appliance by Using the CLI

You can use the CLI installer to perform an unattended upgrade of a vCenter Server appliance or Platform Services Controller appliance. You must run the CLI upgrade from a Windows, Linux, or Mac machine that is in the same network as the appliance that you want to upgrade.

- See Prerequisites for Upgrading the vCenter Server Appliance.
- Prepare Your JSON Configuration File for CLI Upgrade.
- Review the arguments for running the CLI upgrade. See Syntax of the CLI Upgrade Command.

- Verify that the user name with which you are logged in to your machine, the path to the vCenter Server appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file contain only ASCII characters. Extended ASCII and non-ASCII characters are not supported.

1. Navigate to the `vcsa-cli-installer` subdirectory for your operating system.
   - If you are running the upgrade on Windows, navigate to the `vcsa-cli-installer\win32` directory.
   - If you are running the upgrade on Linux, navigate to the `vcsa-cli-installer/lin64` directory.
   - If you are running the upgrade on Mac, navigate to the `vcsa-cli-installer/mac` directory.
2. Optional: Verify that you prepared the upgrade template correctly by running a basic template verification.

   ```
   vcsa-deploy upgrade --verify-template-only path_to_the_json_file
   ```
3. Optional: Gather and validate the upgrade requirements by running a pre-upgrade check.

   ```
   vcsa-deploy upgrade --precheck-only path_to_the_json_file
   ```

   The pre-upgrade check installs the Upgrade Runner on the source appliance that you want to upgrade without upgrading the appliance.

   The Upgrade Runner validates the configurations such as ESXi, network settings, and NTP servers. The Upgrade Runner also checks if you have selected a suitable deployment size and storage size for the new appliance against the compute resources required for the upgrade.
4. Perform the upgrade by running the following command.

   ```
   vcsa-deploy upgrade --accept-eula optional_argumentspath_to_the_json_file
   ```

   Use *optional_arguments* to enter space-separated arguments to set additional execution parameters of the upgrade command.

   For example, you can set the location of the log and other output files that the installer generates. This example also confirms participation in the VMware Customer Experience Improvement Program (CEIP). If the `ceip_enabled` parameter is set to true in the JSON deployment template, you must include the argument `--acknowledge-ceip`.

   ```
   vcsa-deploy upgrade --accept-eula --acknowledge-ceip --log-dir=path_to_the_locationpath_to_the_json_file
   ```

Verify Your vCenter Server Upgrade or Migration Is Successful.

Related Links

Syntax of the CLI Upgrade Command on page 1366

You can use command arguments to set the execution parameters of the upgrade command.

Syntax of the CLI Upgrade Command

You can use command arguments to set the execution parameters of the upgrade command.

You can add a space-separated list of arguments to the CLI upgrade command.

```
vcsa-deploy upgrade path_to_the_json_filelist_of_arguments
```

Argument	Description
`--accept-eula`	Accepts the end-user license agreement. Required for executing the deployment command.
`--acknowledge-ceip`	Confirms your acknowledgement of your VMware Customer Experience Improvement Program (CEIP) participation. Required if the `ceip_enabled` parameter is set to `true` in the JSON deployment template.
`-v`, `--verbose`	Adds debug information to the console output.

Argument	Description
`-t`, `--terse`	Hides the console output. Displays only warning and error messages.
`--log-dir` *`LOG_DIR`*	Specifies the location of the log and other output files that the installer generates.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters and deploys the vCenter Server appliance, but does not validate the OVF Tool parameters in the `ovftool_arguments` subsection of the JSON template. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
`--no-ssl-certificate-verification`	Prohibits SSL verification of for all server connections. The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI stops the upgrade unless you specify that the CLI ignore the self-signed certificate using the `--no-ssl-certificate-verification` command parameter. If you are connecting to a server with a self-signed certificate, and fail to specify that the CLI accept it, the CLI displays the server's self-signed certificate thumbprint, and prompts you to accept or reject the it. You can also specify that the CLI ignore self-signed certificates using the `ssl_certificate_verification` configuration parameter in the JSON template. See Upgrade Configuration Parameters for CLI Upgrade of vCenter Server Appliance . **Important:** Avoid using this option as it may cause problems during or after upgrade due to an un-validated identity of the target host.
`--operation-id`	Lets you provide an identifier to track the concurrent installation, migration, or upgrade of multiple vCenter Server instances. If do not provide an operation ID, the CLI generates a universally unique identifier (UUID) which you can use to identify the different instances of vCenter Server and their installation or upgrade status.
`--pause-on-warnings`	Pauses and waits for acknowledgment of warnings.
`--verify-template-only`	Performs basic template verification without installing Upgrade Runner, running prechecks, and upgrading or migrating the vCenter Server Appliance.
`--precheck-only`	Installs Upgrade Runner on the source appliance and runs a complete set of prechecks without performing the upgrade.
`-h`, `--help`	Displays the help message for the `vcsa-deploy upgrade` command.
`--template-help`	Displays the help message for the use of configuration parameters in the JSON upgrade file.

After the execution finishes, you can get the exit code of the command.

Exit Code	Description
0	Command ran successfully

Exit Code	Description
1	Runtime error
2	Validation error
3	Template error

Related Links

Upgrade a vCenter Server Appliance by Using the CLI on page 1365

You can use the CLI installer to perform an unattended upgrade of a vCenter Server appliance or Platform Services Controller appliance. You must run the CLI upgrade from a Windows, Linux, or Mac machine that is in the same network as the appliance that you want to upgrade.

Migrating vCenter Server for Windows to Appliance

You can migrate a vCenter Server installation on Windows to a appliance installation while upgrading to version 7.0.

Overview of Migration from vCenter Server on Windows to vCenter Server Appliance

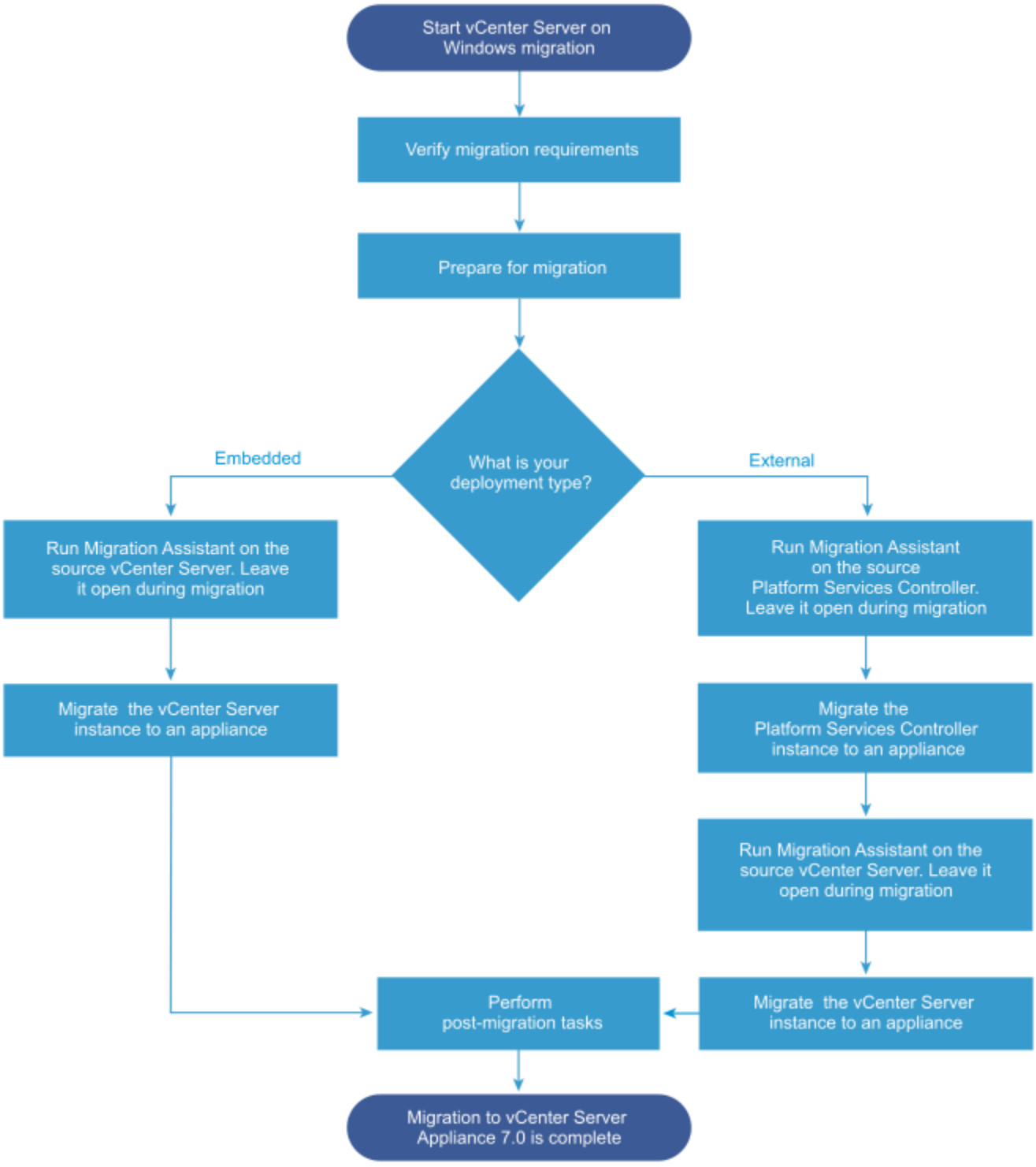
VMware provides supported paths for migrating from vCenter Server version 6.5 and version 6.7 installations on Windows to vCenter Server Appliance7.0 installations.

You can migrate the following deployments:

Table 76: Supported vSphere Migration Paths

Source Configuration	Target Configuration
vCenter Server 6.5 with an Platform Services Controller embedded instance on Windows	vCenter Server Appliance7.0
vCenter Server 6.7 with an embedded Platform Services Controller instance on Windows	
vCenter Server 6.5 instance on Windows	
vCenter Server 6.7 instance on Windows	

Figure 37: High-level Tasks for vCenter Server on Windows Migration to vCenter Server Appliance7.0



You can use the GUI method or the CLI method to migrate your vCenter Server installation from Windows to an appliance.

- GUI Migration of vCenter Server with an Embedded Platform Services Controller to an vCenter Server Appliance

- GUI Migration of vCenter Server with an External Platform Services Controller to an Appliance
- CLI Migration of a vCenter Server Installation from Windows to an Appliance

Important: You cannot change your deployment type during migration.

Migration of Update Manager from Windows to a vCenter Server Appliance 7.0

For vSphere 6.5 and later releases, Update Manager is delivered as a 64-bit application and can be installed only on a 64-bit Windows operating system. In vSphere 6.5 and 6.7, Update Manager is provided as an optional service in vCenter Server Appliance 6.7. VMware provides supported paths for migrating Update Manager from a Windows operating system to a vCenter Server appliance version 7.0. In vSphere 7.0, Update Manager functionality is delivered as part of vSphere Lifecycle Manager.

You can migrate Update Manager in the following vCenter Server deployments:

Table 77: Supported Migration Paths for Update Manager That Runs on Windows to a vCenter Server Appliance

Source Configuration	Target Configuration
vCenter Server and Update Manager run on the same Windows machine	vCenter Server appliance 7.0 with embedded vSphere Lifecycle Manager
vCenter Server and Update Manager run on different Windows machines	vCenter Server appliance 7.0 with embedded vSphere Lifecycle Manager
Update Manager run on a Windows machine and is connected to a vCenter Server Appliance	vCenter Server appliance 7.0 with embedded vSphere Lifecycle Manager

You can use the GUI method or the CLI method to migrate your vCenter Server deployment that uses external Update Manager instance. If you use the GUI method, perform manual steps on the Update Manager Windows system. If you use the CLI method, add configuration parameters about Update Manager in your JSON template.

Important: Verify that the Update Manager source machine does not run additional extensions that are connected to other vCenter Server systems, which are not part of your migration.

Before the migration, Update Manager might use any of the supported Microsoft SQL Server, Oracle, or embedded database solutions. After the migration to the vCenter Server appliance, Update Manager is upgraded to embedded vSphere Lifecycle Manager, which uses the PostgreSQL database.

System Requirements for Migrating vCenter Server Deployments to Appliance Deployments

Your source and target systems must meet specific software and hardware requirements before you can migrate a vCenter Server, vCenter Single Sign-On, or Platform Services Controller deployment to a appliance.

Source System

- Synchronize the clocks on all machines running the source vCenter Server services. See Synchronizing Clocks on the vSphere Network.
- Verify that your vCenter Server and Platform Services Controller certificates are valid for the vCenter Server or Platform Services Controller and have not expired.
- Verify that the system network name of the machines running the target vCenter Server services are valid, and are reachable from other machines in the network.
- Verify that the host name of the virtual machine or physical server from which you are migrating vCenter Server complies with RFC 1123 guidelines.

- If your vCenter Server service is running in a user account other than the Local System account, verify that the user account in which the vCenter Server service is running has the following permissions:
  - **Member of the Administrators group**
  - **Log on as a service**
  - **Act as part of the operating system (if the user is a domain user)**
  - **Replace a process level token**
- Verify that the LOCAL SERVICE account has read permission on the folder in which vCenter Server is installed and on the HKLM registry.
- Verify that the connection between the virtual machine or physical server and the domain controller is working.
- Verify that the source vCenter Server instance or Platform Services Controller instance on Windows does not use a DHCP IP address as its system network name.

  Important: Migration from a source Windows machine using a DHCP IP Address as its system network name to an appliance is not supported.

Target System

- Your target system must meet specific software and hardware requirements for appliance. See System Requirements for the vCenter Server Appliance.
- When you use Fully Qualified Domain Names, make sure that the machine you use for deploying the appliance and the target ESXi host or vCenter Server instance are on the same DNS server.
- Synchronize the clocks of all target virtual machines on the vSphere network before beginning migration. Unsynchronized clocks might result in authentication problems and can cause the migration to fail or prevent the vCenter Server services from starting. See Synchronizing Clocks on the vSphere Network.

Pre-migration Checks

When you migrate vCenter Server for Windows to vCenter Server Appliance, the upgrade installer performs a pre-check of the environment to ensure it meets requirements. For example, the pre-check verifies that enough space is available on the virtual machine or physical server where you are migrating, and that the external database, if any, can be successfully accessed.

Source Environment Checks

When you migrate vCenter Server for Windows versions 6.5 or 6.7, vCenter Single Sign-On is included as part of the Platform Services Controller. When you provide the information about the vCenter Single Sign-On service, the installer uses the administrator account to check the host name and password, to verify that the details of the vCenter Single Sign-On server you provided can be authenticated before proceeding with the migration process.

The pre-migration checker performs checks for the following aspects of the source environment:

- vCenter Server or Platform Services Controller to verify that migration is supported
- SSL certificates validity and compatibility with system names
- Network connections
- DNS resolution
- Internal and external ports used
- External database connectivity
- Administrator privileges on the Windows machine
- Required disk space for exporting configuration data
- NTP server validation
- Any credentials that you enter

Target Environment Checks

The pre-migration checker performs checks for the following aspects of the target environment:

- Minimum processor requirements
- Minimum memory requirements
- Minimum disk space requirements
- Administrator privileges on the target host
- Any credentials that you enter

Known Limitations

The current release has several known limitations.

The following list contains features or actions that are currently not supported:

- Local Windows OS users and groups are not migrated to the Photon OS of the 7.0. If you assigned vCenter Server permissions to any Local Windows OS users and groups, remove the permissions assignments before the migration. You can re-create Local OS users and groups on the Photon OS of the 7.0 after the migration.
- After the migration, the source vCenter Server is turned off and cannot be turned on to avoid network ID conflicts with the target appliance. After the source vCenter Server is turned off, all solutions that are installed on the source vCenter Server and that are not migrated become unavailable.
- Migration of deployments that use custom ports for services other than Auto Deploy, Update Manager, vSphere ESXi Dump Collector, and HTTP reverse proxy (RHTTP) are not supported.
- The migration process migrates only one network adapter setting to the target appliance. If the hostname of the source vCenter Server resolves to multiple IP addresses across multiple network adapters, you can select which IP address and network adapter settings to migrate. You cannot add the rest of the network adapters and settings to the target appliance.

Preparing for Migration

Before beginning to migrate any type of vCenter Server deployment to an appliance, you must complete the preparation tasks.

Preparation tasks:

- Synchronizing Clocks on the vSphere Network
- Preparing vCenter Server Databases for Migration
- Prepare Managed ESXi Hosts for Migration
- Download and Mount the vCenter Server Installer
- Download and Run VMware Migration Assistant on the Source Windows Machine

Synchronizing Clocks on the vSphere Network

Verify that all components on the vSphere network have their clocks synchronized. If the clocks on the physical machines in your vSphere network are not synchronized, SSL certificates and SAML tokens, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server`vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause the first boot of a component in your environment to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server is not synchronized with NTP or PTP.

Similarly, issues can arise if the destination vCenter Server migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server instance.

- The target ESXi host where the destination vCenter Server is to be deployed is synchronized to NTP or PTP.
- The ESXi host running the source vCenter Server is synchronized to NTP or PTP.
- When upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, if the vCenter Server appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP or PTP.
- If you are upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, verify that the source vCenter Server or vCenter Server appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the VMware knowledge base article at https://kb.vmware.com/s/article/1318.

To synchronize ESXi clocks with an NTP or a PTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see topic *Edit the Time Configuration of an ESXi Host in the VMware Host Client* in the *vSphere Single Host Management - VMware Host Client* documentation.

To learn how to change time synchronization settings for vCenter Server, see topic *Configure the System Time Zone and Time Synchronization Settings* in the *vCenter Server Configuration* documentation.

To learn how to edit the time configuration for a host by using the vSphere Client, see topic *Editing the Time Configuration Settings of a Host* in the *vCenter Server and Host Management* documentation.

Synchronize ESXi Clocks with a Network Time Server

Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

This task explains how to set up NTP from the VMware Host Client. You can instead use the `vicfg-ntp` vCLI command. See the *vSphere Command-Line Interface Reference*.

1. Start the VMware Host Client, and connect to the ESXi host.
2. Click **Configure**.
3. Under **System**, click **Time Configuration**, and click **Edit**.
4. Select **Use Network Time Protocol (Enable NTP client)**.
5. In the Add NTP Server text box, enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.
6. Optional: Set the startup policy and service status.
7. Click **OK**.

   The host synchronizes with the NTP server.

Related Links

Configuring Time Synchronization Settings in vCenter Server on page 1722

You can change the time synchronization settings in vCenter Server after deployment.

Preparing vCenter Server Databases for Migration

The appliance instance requires a database to store and organize server data. Ensure your source vCenter Server database is prepared for migration to the target appliance.

Each appliance instance must have its own database. The bundled PostgreSQL database that is included in the appliance supports up to 2,500 hosts and 30,000 virtual machines.

To ensure your database is prepared for migration:

- Verify that passwords are current and not set to expire soon.
- Reduce the database size. For more information, see Knowledge Base article KB 2110031.
- Verify that you have backed up your database. See your database documentation.
- Verify that vCenter Server can communicate with the local database.

During the migration of vCenter Server to appliance, the installer:

1. Exports the vCenter Server database.
2. Deploys the target appliance in an unconfigured state.
3. Copies exported data to the target appliance.
4. Starts the PostgreSQL service to import the source database data.
5. Upgrades the database schema to be compatible with the target appliance.
6. Starts the target appliance services.

When you configure the target appliance, you initialize and configure using the imported database with the old schema. You have a choice of migration options:

1. Inventory tables
2. Inventory tables with events and tasks
3. All database data

Prepare an Oracle Database for Migration

Ensure that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before migrating your Oracle database from Windows to an embedded PostgreSQL database in the appliance.

Verify that you have confirmed basic interoperability before preparing your Oracle database for migration.

Verify that you have backed up your database. For information about backing up the vCenter Server database, see the Oracle documentation.

1. Verify that passwords are current and not set to expire soon.
2. Ensure that you have login credentials, the database name, and the database server name that the vCenter Server database is to use.

   Look in the ODBC system for the connection name of the database source name for the vCenter Server database.
3. Use the Oracle SERVICE_NAME instead of SID to verify that your Oracle database instance is available.
   - Log in to the database server to read from the alert log: `$ORACLE_BASE/diag/rdbms/$instance_name/$INSTANCE_NAME/trace/alert_$ INSTANCE_NAME.log`.
   - Log in to the database server to read from the Oracle Listener status output.
   - If you have the SQL*Plus client installed, you can use `tnsping` for the vCenter Database instance. If the `tnsping` command does not work the first time, retry it after waiting a few minutes. If retrying does not work, restart the vCenter Database instance on the Oracle server and then retry `tnsping` to ensure it is available.
4. Verify that the JDBC driver file is included in the CLASSPATH variable.
5. Verify that permissions are set correctly.
6. Either assign the DBA role or grant the required permissions to the user.
7. Make a full backup of the vCenter Server database.

Your database is prepared for the vCenter Server migration to vCenter Server Appliance.

Prepare a Microsoft SQL Server Database for Migration

Ensure that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before migrating your Microsoft SQL Server database on Windows to an embedded PostgreSQL database appliance.

Verify that you have backed up your database. For information about backing up the vCenter Server database, see the Microsoft SQL Server documentation.

Important: You cannot use Integrate Windows for your authentication method if the vCenter Server service is running under the Microsoft Windows built-in system account.

1. Verify that passwords are current and not set to expire soon.
2. Verify that JDK 1.6 or later is installed on the vCenter Server machine.
3. Verify that the `sqljdbc4.jar` file is added to the CLASSPATH variable on the machine where vCenter Server Appliance is to be migrated.

   If the `sqljdbc4.jar` file is not installed on your system, the vCenter Server Appliance installer installs it.
4. Verify that your system database source name is using the Microsoft SQL Server Native Client 10 or 11 driver.
5. Make a full backup of the vCenter Server database.

Your database is prepared for the vCenter Server migration to vCenter Server Appliance.

Prepare PostgreSQL Database Before Migrating vCenter Server to an Appliance

Ensure that you have the necessary credentials, and that you complete any necessary cleanup or other preparation before migrating your PostgreSQL database installation on Windows to an appliance.

Verify that you have confirmed basic migration interoperability before preparing your PostgreSQL database for migrating vCenter Server.

For information about backing up the vCenter Server database, see the PostgreSQL documentation.

1. Verify that passwords are current and not set to expire soon.
2. For vCenter Server, locate the `cleanup_orphaned_data_PostgresSQL.sql` script in the ISO image and copy it to your PostgreSQL server.
3. Log in to vCenter Server Appliance as root user.
4. Run the cleanup script.
   /opt/vmware/vpostgres/9.4/bin/psql -U postgres -d VCDB -f *path* cleanup_orphaned_data_Postgres.sql

   The cleanup script cleans and purges any unnecessary or orphaned data in your vCenter Server database that is not used by any vCenter Server component.
5. Make a full backup of the vCenter Server database.

Your database is prepared for the vCenter Server migration to vCenter Server Appliance.

Prepare Managed ESXi Hosts for Migration

You must prepare the ESXi hosts managed by your vCenter Server installation before migrating it from Windows to vCenter Server7.0.

To migrate vCenter Server or an external Platform Services Controller from Windows to vCenter Server7.0, your source and target ESXi hosts must meet the migration requirements.

- ESXi hosts must be at version 6.5 or greater. For information on ESXi compatibility, see the VMware Compatibility Guide.
- ESXi hosts must not be in lockdown or maintenance mode.

1. To keep your current SSL certificates, back up the SSL certificates that are on the vCenter Server system before you upgrade to vCenter Server7.0.

   The default location of the SSL certificates is `%allusersprofile%\VMware\VMware VirtualCenter`.
2. If you have Custom or Thumbprint certificates, see Host Upgrades and Certificates to determine your preparatory steps.
3. If you have vSphere HA clusters, SSL certificate checking must be enabled.

   If you have vSphere HA clusters, SSL certificate checking must be enabled.

   a) Select the vCenter Server instance in the vSphere Client inventory tree.
   b) Select the **Manage** tab and the **General** subtab.
   c) Verify that **vCenter Server requires verified host SSL certificates** is selected.

Your ESXi hosts are ready for migration to the vCenter Server appliance.

Preparing vCenter Server Certificates for Migration

You must verify that your source vCenter Server certificates are prepared before you start the migration process.

In vSphere 6.0 and later certificates are stored in the VMware Endpoint Certificate Store. The migration process proceeds normally and preserves your certificates. For information about vCenter Server certificate locations, see Knowledge Base article KB 2111411.

Certificate Files Location

The vCenter Server certificate files are located at `%ProgramData%\VMware\VMware VirtualCenter\SSL`

Supported Certificate Types

If your environment uses any of the supported certificate types, you can continue with the migration. The migration process proceeds normally and preserves your certificates.

- Your `rui.crt` file contains the entire chain including the leaf certificate. You can create this type of certificate by deploying and using the VMware SSL Certificate Automation Tool, see see Knowledge Base article KB 2057340 .
- Your `rui.crt` file contains the leaf certificate and the corresponding `cacert.pem` is available in `%ProgramData%\VMware\VMware VirtualCenter\SSL` to validate the `rui.crt`.

Unsupported Certificate Types

If your environment uses any of the unsupported certificate types, you must prepare your certificates before you can proceed with the migration process proceeds.

- Your `rui.crt` contains only the leaf certificate, the `cacert.pem` is missing or invalid, and `cacert.pem` is not added to the Windows trust store.

  Get the Certificate Authority certificate, including all intermediate certificates, and create a `cacert.pem` file, or replace the vCenter Server certificates with any of the supported formats.
- Your `rui.crt` contains only the leaf certificate and the `cacert.pem` is missing or invalid, but the `cacert.pem` is added to the Windows trust store.

  Get the Certificate Authority certificate, including all intermediate certificates from the Windows trust store and create `cacert.pem`. Use OpenSSL to verify the certificate by running `verify -CAfile cacert.pem rui.crt` command.

For more information about vSphere security certificates, see the *vSphere Security* documentation.

System Requirements for the vCenter Server Installer

You can run the vCenter Server GUI or CLI installer from a network client machine that is running on a Windows, Linux, or Mac operating system of a supported version.

To ensure optimal performance of the GUI and CLI installers, use a client machine that meets the minimum hardware requirements.

Table 78: System Requirements for the GUI and CLI Installers

Operating System	Supported Versions	Minimum Hardware Configuration for Optimal Performance
Windows	• Windows 8, 8.1, 10 • Windows 2012 x64 bit • Windows 2012 R2 x64 bit • Windows 2016 x64 bit • Windows 2019 x64	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC
Linux	• SUSE 15 • Ubuntu 16.04 and 18.04	4 GB RAM, 1 CPU having 2 cores with 2.3 GHz, 16 GB hard disk, 1 NIC **Note:** The CLI installer requires 64-bit OS.
Mac	• macOS v10.13, 10.14, 10.15 • macOS High Sierra, Mojave, Catalina	8 GB RAM, 1 CPU having 4 cores with 2.4 GHz, 150 GB hard disk, 1 NIC

Note: For client machines that run on Mac 10.13 or later, concurrent GUI deployments of multiple appliances are unsupported. You must deploy the appliances in a sequence.

Note: Visual C++ redistributable libraries need to be installed to run the CLI installer on versions of Windows older than Windows 10. The Microsoft installers for these libraries are located in the `vcsa-cli-installer/win32/vcredist` directory.

Note: Deploying the vCenter Server appliance with the GUI requires a minimum resolution of 1024x768 to properly display. Lower resolutions can truncate the UI elements.

Determine the Oracle Database Size and the Storage Size for the New Appliance

Before upgrading a vCenter Server appliance or migrating a vCenter Server on Windows that uses an external Oracle database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new vCenter Server appliance database using an embedded PostgreSQL database.

You must have the vCenter Server database login credentials.

You run scripts to determine the Oracle core table size, the events and tasks table size, and the statistics table size. The Oracle core table corresponds to the database (`/storage/db`) partition of the PostgreSQL database. The Oracle events and tasks and statistics tables correspond to the statistics, events, alarms, and tasks (`/storage/seat`) partition of the PostgreSQL database.

During the upgrade of the appliance, you must select a storage size for the new appliance that is at least twice the size of the Oracle tables size.

During the upgrade of the appliance, you can select the types of data to transfer to the new appliance. To minimize upgrade time and storage requirements for the new appliance, you can choose to transfer only the configuration data.

1. Log in to a SQL*Plus session with the vCenter Server database user.
2. Determine the core table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
  FROM   user_segments s
  WHERE  (s.segment_name,s.segment_type)
               IN (SELECT seg_name, seg_type FROM
                       (SELECT t.table_name seg_name, t.table_name tname,
                         'TABLE' seg_type
                         FROM   user_tables t
                        UNION
                        SELECT i.index_name, i.table_name,
                        'INDEX'
                         FROM   user_indexes i
                       ) ti
                   WHERE  (ti.tname LIKE 'VPX_%'
                           OR ti.tname LIKE 'CL_%'
                           OR ti.tname LIKE 'VDC_%')
                       AND ti.tname NOT LIKE 'VPX_SAMPLE_TIME%'
                       AND ti.tname NOT LIKE 'VPX_HIST_STAT%'
                       AND ti.tname NOT LIKE 'VPX_TOPN%'
                       AND ti.tname NOT LIKE 'VPX_SDRS_STATS_VM%'
                       AND ti.tname NOT LIKE 'VPX_SDRS_STATS_DATASTORE%'
                       AND ti.tname NOT LIKE 'VPX_TASK%'
                       AND ti.tname NOT LIKE 'VPX_EVENT%'
                       AND ti.tname NOT LIKE 'VPX_PROPERTY_BULLETIN%');
```

   The script returns the database storage size in MB.

3. Determine the events and tasks table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
             IN (SELECT seg_name, seg_type FROM
                     (SELECT t.table_name seg_name, t.table_name tname,
                       'TABLE' seg_type
                       FROM   user_tables t
                      UNION
                      SELECT i.index_name, i.table_name,
                      'INDEX'
                       FROM   user_indexes i
                     ) ti
                 WHERE
                    ti.tname LIKE 'VPX_TASK%'
                 OR ti.tname LIKE 'VPX_EVENT%');
```

   The script returns the events and tasks storage size in MB.

4. Determine the statistics table size by running the following script.

```
SELECT ROUND(SUM(s.bytes)/(1024*1024)) SIZE_MB
FROM   user_segments s
WHERE  (s.segment_name,s.segment_type)
```

```
IN (SELECT seg_name, seg_type FROM
         (SELECT t.table_name seg_name, t.table_name tname,
           'TABLE' seg_type
           FROM   user_tables t
          UNION
          SELECT i.index_name, i.table_name,
          'INDEX'
           FROM   user_indexes i
         ) ti
    WHERE
       ti.tname LIKE 'VPX_SAMPLE_TIME%'
    OR ti.tname LIKE 'VPX_TOPN%'
    OR ti.tname LIKE 'VPX_TASK%'
    OR ti.tname LIKE 'VPX_EVENT%'
    OR ti.tname LIKE 'VPX_HIST_STAT%');
```

The script returns the statistics storage size in MB.

5. Calculate the minimum storage size for the new appliance that you are going to deploy during the upgrade.
   a) The size of the database (`/storage/db`) partition of the embedded PostgreSQL database must be at least twice the size of the Oracle core table returned in 2.
   b) The size of the statistics, events, alarms, and tasks (`/storage/seat`) partition of the embedded PostgreSQL database must be at least twice the sum of the sizes of the Oracle events and tasks and statistics tables returned in 3 and 4.

   For example, if the Oracle core table is 100 MB, the events and tasks table is 1,000 MB, and the statistics table is 2,000 MB, then the Postgres `/storage/db` partition must be at least 200 MB and the `/storage/seat` partition must be at least 6,000 MB.

Related Links

Storage Requirements for the vCenter Server Appliance on page 1246

When you deploy the vCenter Server appliance, the ESXi host or DRS cluster on which you deploy the appliance must meet minimum storage requirements. The required storage depends not only on the size of the vSphere environment and the storage size, but also on the disk provisioning mode.

Determine the Microsoft SQL Server Database Size and the Storage Size for the New vCenter Server Appliance

Before upgrading a vCenter Server appliance, or migrating a vCenter Server on Windows that uses an external Microsoft SQL Server database, you must determine the size of the existing database. Based on the size of the existing database, you can calculate the minimum storage size for the new vCenter Server appliance. This storage size allows the embedded PostgreSQL database to assume the data from the old database with enough free disk space after the upgrade.

You must have the vCenter Server database login credentials.

You run scripts to determine the Microsoft SQL Server core table size, the events and tasks table size, and the statistics table size. The Microsoft SQL Server core table corresponds to the database (`/storage/db`) partition of the PostgreSQL database. The Microsoft SQL Server events and tasks and statistics tables correspond to the statistics, events, alarms, and tasks (`/storage/seat`) partition of the PostgreSQL database.

During the upgrade of the appliance, you must select a storage size for the new appliance that is at least twice the size of the Microsoft SQL Server tables size.

1. Log in to a SQL Management Studio session with the vCenter Server database user.
2. Determine the core table size by running the following script.

```
SELECT SUM(p.used_page_count * 8)/1024 AS disk_size
```

```
 FROM sys.dm_db_partition_stats p
 JOIN sys.objects o
   ON o.object_id = p.object_id
WHERE o.type_desc = 'USER_TABLE'
  AND o.is_ms_shipped = 0 AND UPPER(o.name) NOT LIKE 'VPX_HIST_STAT%'
  AND UPPER(o.name) NOT LIKE 'VPX_SAMPLE_TIME%'
  AND UPPER(o.name) NOT LIKE 'VPX_TOPN%'
  AND UPPER(o.name) NOT LIKE 'VPX_TASK%'
  AND UPPER(o.name) NOT LIKE 'VPX_EVENT%'
  AND UPPER(o.name) NOT LIKE 'VPX_SDRS_STATS_VM%'
  AND UPPER(o.name) NOT LIKE 'VPX_SDRS_STATS_DATASTORE%'
  AND UPPER(o.name) NOT LIKE 'VPX_PROPERTY_BULLETIN%';
```

The script returns the database storage size in MB.

3. Determine the events and tasks table size by running the following script.

```
SELECT SUM(p.used_page_count * 8)/1024 AS disk_size
  FROM sys.dm_db_partition_stats p
  JOIN sys.objects o
    ON o.object_id = p.object_id
 WHERE o.type_desc = 'USER_TABLE'
   AND o.is_ms_shipped = 0 AND ( UPPER(o.name) LIKE 'VPX_TASK%'
    OR UPPER(o.name) LIKE 'VPX_EVENT%');
```

The script returns the events and tasks storage size in MB.

4. Determine the statistics table size by running the following script.

```
SELECT SUM(p.used_page_count * 8)/1024 AS disk_size
  FROM sys.dm_db_partition_stats p
  JOIN sys.objects o
    ON o.object_id = p.object_id
 WHERE o.type_desc = 'USER_TABLE'
   AND o.is_ms_shipped = 0
   AND (     UPPER(o.name) LIKE 'VPX_HIST_STAT%'
         OR UPPER(o.name) LIKE 'VPX_SAMPLE_TIME%'
         OR UPPER(o.name) LIKE 'VPX_TOPN%');
```

The script returns the statistics storage size in MB.

5. Calculate the minimum storage size for the new appliance that you are going to deploy during the upgrade.
   a) The size of the database (`/storage/db`) partition of the embedded PostgreSQL database must be at least twice the size of the Microsoft SQL Server core table returned in 2.
   b) The size of the statistics, events, alarms, and tasks (`/storage/seat`) partition of the embedded PostgreSQL database must be at least twice the sum of the sizes of the Microsoft SQL Server events and tasks and statistics tables returned in 3 and 4.

   For example, if the Microsoft SQL Server core table is 100 MB, the events and tasks table is 1,000 MB, and the statistics table is 2,000 MB, then the Postgres `/storage/db` partition must be at least 200 MB and the `/storage/seat` partition must be at least 6,000 MB.

Download and Run VMware Migration Assistant on the Source Windows Machine

You must download and run the VMware Migration Assistant on your source vCenter Server or Platform Services Controller to prepare it for migration from Windows to a vCenter Server appliance. If your deployment of vCenter Server has an external Update Manager that runs on Windows, download and run the VMware Migration Assistant on the source

Windows machine. Update Manager prepares the Update Managerserver and database for migration from Windows to the vCenter Server appliance.

- Download and Mount the vCenter Server Installer.
- Log in to the Windows machine as an administrator.

The VMware Migration Assistant performs the following tasks on the source Windows machine where you run it:

1. Discovers the source deployment type.
2. Runs pre-checks on the source.
3. Reports errors that must be addressed before starting the migration.
4. Provides information for the next steps in the migration process.

Ensure that the VMware Migration Assistant window remains open during the migration process. Closing the VMware Migration Assistant causes the migration process to stop.

1. In the vCenter Server appliance installer package, locate the directory that contains VMware Migration Assistant.
2. Copy the VMware Migration Assistant folder to the source Windows machine where either one of the following components runs:
   - Update Manager
   - Platform Services Controller
   - vCenter Server

   CAUTION: If Update Manager runs on a different Windows machine than any other of the vCenter Server components that you are migrating, run VMware Migration Assistant on the Update Manager source machine first. If you do not run VMware Migration Assistant on the Update Manager source machine first, the VMware Migration Assistant on vCenter Server may fail.
3. Run the VMware Migration Assistant on the Windows machine.
   - For the GUI, double-click `VMware-Migration-Assistant.exe`
   - For the CLI, enter: `VMware-Migration-Assistant.exe -p <password of Administrator@vmdir.domain>`

     To list all the available input parameters, enter: `VMware-Migration-Assistant.exe --help`.

   Important: Leave the Migration Assistant window open until you finish the upgrade or the migration process of your vCenter Server deployment.

   The VMware Migration Assistant runs pre-upgrade checks and prompts you to resolve any errors it finds before proceeding with the migration.

When the pre-checks are finished and any errors are addressed, your source system is ready for migration.

To begin the migration process, follow the VMware Migration Assistant instructions.

For detailed migration steps, see one of the following.

- GUI Migration of vCenter Server with an Embedded Platform Services Controller to an vCenter Server Appliance
- GUI Migration of vCenter Server with an External Platform Services Controller to an Appliance
- CLI Migration of a vCenter Server Installation from Windows to an Appliance

Prerequisites for Migrating vCenter Server

To ensure the successful migration of vCenter Server, you must perform a set of required tasks and pre-checks prior to running the migration.

General Prerequisites

- Download and Mount the vCenter Server Installer.
- Verify that the clocks of all machines on the vSphere network are synchronized. See Synchronizing Clocks on the vSphere Network.

Target System Prerequisites

- Verify that your system meets the minimum software and hardware requirements. See System Requirements for the vCenter Server Appliance.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on an ESXi host, verify that the target ESXi host is not part of a fully automated DRS cluster.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster contains at least one ESXi host that is not in lockdown or maintenance mode.
- If you plan to deploy the new appliance on a DRS cluster of the inventory of a vCenter Server instance, verify that the cluster is not fully automated.

Source System Prerequisites

- Verify that the source machine that you want to migrate does not run on an ESXi host that is part of a fully automated DRS cluster.
- Verify that you have sufficient disk space on the source machine that you want to migrate so that you can accommodate the data for the migration.
- Create an image-based backup of the vCenter Server appliance you are migrating as a precaution in case there is a failure during the migration process. If you are migrating a vCenter Server appliance with an external Platform Services Controller, take a image-based backup of the Platform Services Controller appliance as well.

  Important: To take a pre-migration image-based backup, power off all the vCenter Server and Platform Services Controller nodes in your environment, and take a backup of each node. After you have taken backups of all the nodes, you can restart them and proceed with the migration procedure.

  If the migration fails, delete the newly deployed vCenter Server appliance, and restore the vCenter Server and Platform Services Controller nodes from their respective backups. You must restore all the nodes in the environment from their backups. Failing to do so will cause the replication partners to be out of synchronization with the restored node.

  To learn about image-based back, see "Image-Based Backup and Restore of a vCenter Server Environment" in *vCenter Server Installation and Setup*.
- If you use an external database, back up the external database.

Network Prerequisites

- If you plan to assign a static IP address in the temporary network settings of the appliance, verify that you have configured the forward and reverse DNS records for the IP address.
- If you plan to assign a DHCP IP address in the temporary network settings of the new appliance, verify that the ESXi host on which you want to deploy the new appliance is in the same network as the ESXi host on which the existing vCenter Server appliance runs.
- If you plan to assign a DHCP IP address in the temporary network settings of the new appliance, verify that the ESXi host on which you want to deploy the new appliance is connected to at least one network that is associated with a port group which accepts MAC address changes. Note that the default security policy of a distributed virtual switch is to reject MAC address changes. For information about how to configure the security policy for a switch or port group, see *vSphere Networking*.
- Add the source vCenter Server IP address in the DNS records.

Required Information for Migrating vCenter Server from Windows to an Appliance

The vCenter Server migration wizard prompts you for the deployment and migration information when migrating a vCenter Server instance or a Platform Services Controller instance from Windows to an appliance. It is a best practice to keep a record of the values that you entered in case you must power off the appliance and restore the source installation.

You can use this worksheet to record the information that you need for migrating a vCenter Server instance with a Platform Services Controller from Windows to an appliance.

Important: The user name that you use to log in to the machine from which you want run the GUI installer, the path to the vCenter Server Appliance installer, and your values including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

Local OS users existing on source windows machine are not migrated to the target vCenter Server Appliance and must be recreated after migration is complete. If any local OS user names are used to log in to the vCenter Single Sign-On, you must recreate them and reassign permissions in the Platform Services Controller appliance.

If the source vCenter Server machine is joined to an Active Directory domain, the account you use must have permissions to rejoin the machine to the domain. For more information, see http://kb.vmware.com/kb/2146454.

Table 79: Information Required for Migrating vCenter Server from Windows to vCenter Server Appliance

Required Information		Default Value	Your Entry
Required source vCenter Server migration data	vCenter Server IP address or FQDN		
	vCenter Single Sign-On administrator user name	administrator@vsphere.local **Important:** The user must be administrator@*your_domain_name*.	
	Password of the vCenter Single Sign-On administrator		
	Migration Assistant port number		
	vCenter Server version		
	Temporary upgrade files path	`%LOCALAPPDATA%\VMware\Migration-Assistant\export`	
	IP address or FQDN of the source ESXi host on which the source vCenter Server resides		
	Source ESXi host user name with administrative rights on the source ESXi host		
	Source ESXi host password		
	Migrate performance & other historical data	Disabled by default	
	Migration Assistant thumbprint		
	Active Directory administrator credentials		
	Service account credentials, if vCenter Server is running under a customer user account		

Required Information		Default Value	Your Entry
Required target vCenter Server Appliance data	IP address or FQDN of the target ESXi host or vCenter Server instance where you deploy the new vCenter Server Appliance to which you migrate the source vCenter Server		
	User name with administrative privileges for the target ESXi host or vCenter Server instance, data center or data center folder, and resource pool of an ESXi host or DRS cluster to which to migrate the source installation		
	Password for the target ESXi host. or vCenter Server instance, data center or data center folder, and resource pool of an ESXi host or DRS cluster		
	vCenter Single Sign-On username		
	vCenter Single Sign-On password		
	Target vCenter Server Appliance name		
	Password of the root user		
	vCenter Server Appliance size. The options vary depending on the size of your vSphere environment. • Tiny (up to 10 hosts, 100 virtual machines) • Small (up to 100 hosts, 1,000 virtual machines) • Medium (up to 400 hosts, 4,000 virtual machines) • Large (up to 1,000 hosts, 10,000 virtual machines) • X-Large (up to 2,000 hosts, 35,000 virtual machines)	Tiny (up to 10 hosts, 100 virtual machines)	
	Storage size of the vCenter Server Appliance for your vSphere environment. Increase the default storage size if you want larger volume for SEAT data (stats, events, alarms, and tasks). • Default For tiny deployment size, deploys the appliance with 250 GB of storage. For small deployment size, deploys the appliance with 290 GB of storage. For medium deployment size, deploys the appliance with 425 GB of storage. For large deployment size, deploys the appliance with 640 GB of storage. For x-large deployment size, deploys the appliance with 980 GB of storage.	Default	

Required Information		Default Value	Your Entry
	• Large For tiny deployment size, deploys the appliance with 775 GB of storage. For small deployment size, deploys the appliance with 820 GB of storage. For medium deployment size, deploys the appliance with 925 GB of storage. For large deployment size, deploys the appliance with 990 GB of storage. For x-large deployment size, deploys the appliance with 1030 GB of storage. • X-Large For tiny deployment size, deploys the appliance with 1650 GB of storage. For small deployment size, deploys the appliance with 1700 GB of storage. For medium deployment size, deploys the appliance with 1805 GB of storage. For large deployment size, deploys the appliance with 1870 GB of storage. For x-large deployment size, deploys the appliance with 1910 GB of storage.		
	Name of the datastore on which the new version of the vCenter Server Appliance is deployed		
	Enable or disable thin disk mode.	Disabled by default	
	Join or do not participate in the VMware Customer Experience Improvement Program (CEIP). For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.	Join the CEIP	
Temporary network for communication between the source vCenter Server and the target vCenter Server Appliance	IP address version	IPv4	
	IP address allocation method	DHCP	
Static assignment settings	Network address		
	Subnet mask		
	Network gateway		
	Network DNS servers, separated with commas		
Enable or disable SSH		Disabled by default	

GUI Migration of vCenter Server with an Embedded Platform Services Controller to an vCenter Server Appliance

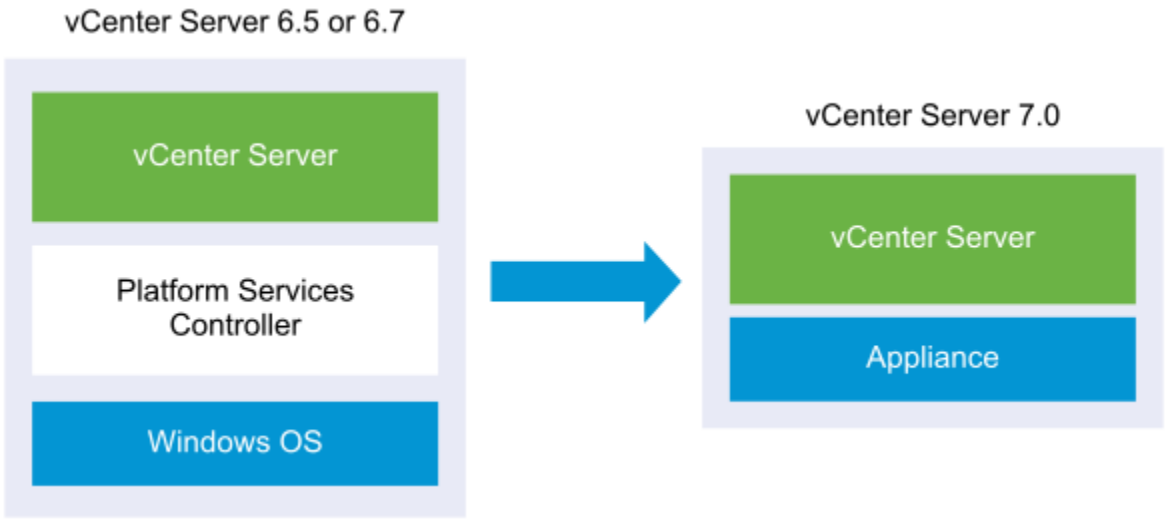
You can use the GUI method to migrate a vCenter Server instance with an embedded Platform Services Controller to a vCenter Server appliance.

When you migrate from vCenter Server with an embedded Platform Services Controller on Windows to vCenter Server appliance, the entire deployment is migrated in a single step.

If you use Update Manager in the deployment on Windows that you migrate, and Update Manager runs on a separate machine from any other of the components, take an extra step to migrate Update Manager to an appliance.

1. If your deployment on Windows uses an external Update Manager, run Migration Assistant on the Update Manager machine to start the migration of the Update Manager server and database to the Update Manager appliance.
2. Migrate the vCenter Server instance with embedded Platform Services Controller from Windows to a vCenter Server appliance.

Figure 38: vCenter Server 6.5 or 6.7 with Embedded Platform Services Controller Deployment Before and After Migration



GUI tasks for migrating vCenter Server with an embedded Platform Services Controller from Windows to a vCenter Server appliance.

1. Download and Mount the vCenter Server Installer ISO file on a network virtual machine or physical server from which you want to perform the migration.
2. Download and Run VMware Migration Assistant on the Source Windows Machine.
   Note: If you are migrating a system that uses an external instance of Update Manager that runs on a separate Windows machine, first run Migration Assistant on the Update Manager machine.
3. Assemble the Required Information for Migrating vCenter Server from Windows to an Appliance.
4. Deploy the OVA File for Migrating to the Target vCenter Server Appliance.
5. Set Up the Target vCenter Server Appliance

Important: The user name that you use to log in to the machine from which you want run the GUI installer, the path to the vCenter Server appliance installer, and your values including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

The installer:

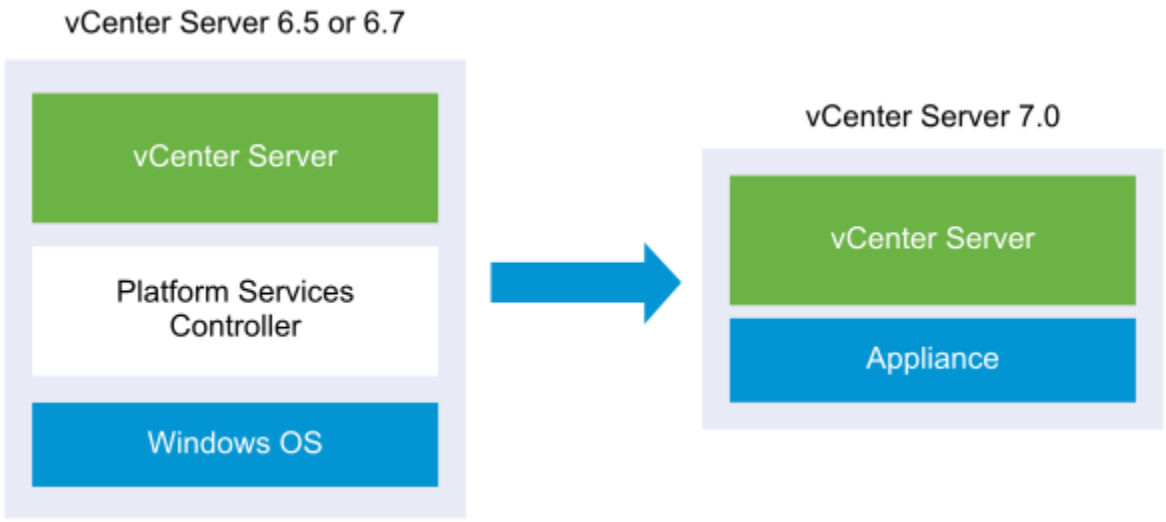
- Deploys a new target appliance.
- Exports the required files from the source vCenter Server.
- Copies the required files to the new vCenter Server appliance.
- Runs the migration process on the new vCenter Server appliance as specified in the Summary.
- Imports and updates the files and settings of the source vCenter Server installation to the new vCenter Server appliance.

Deploy the OVA File for Migrating to the Target vCenter Server Appliance

To start the migration process, you use the GUI installer to deploy the OVA file that is included in the installer ISO file as the target vCenter Server appliance.

- See Prerequisites for Migrating vCenter Server

Figure 39: vCenter Server 6.5 or 6.7 with Embedded Platform Services Controller Deployment Before and After Migration



1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.

2. On the Home page, click **Migrate**.
3. Review the Introduction page to understand the migration process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. On the Connect to source page, enter the details for the source vCenter Server instance, and click **Next**.
   a) Enter the IP address or FQDN.
   b) Enter the user name and password of a user who has administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user.
   c) Enter the Migration Assistant Port you received in the Migration Assistant instructions.
6. Optional: Review the warning message and try to resolve the warnings, if any, and click **Yes**.
7. Connect to the target server to which you want to migrate the source vCenter Server.

Option	Steps
You can connect to an ESXi host on which to deploy the target appliance.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the target appliance.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

8. On the Set up target appliance VM page, enter a name for the target vCenter Server appliance, set the password for the root user, and click **Next**.

   The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sigh (@), or brackets (()).

   Important: The local operating system password is not migrated to the target appliance.
9. Select the deployment size for the new vCenter Server appliance for your vSphere inventory.

   Note: You cannot select a deployment size that is smaller than the source deployment.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory.

Deployment Size Option	Description
	Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

Note: At the bottom of the deployment size table, a row shows the size information of the source machine. This size information is reported by the migration assistant and might help understand why you cannot select some deployment sizes.

10. Select the storage size for the new vCenter Server appliance, and click **Next**.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

11. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.
12. Configure the temporary network for communication between the source vCenter Server and the target vCenter Server appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily.

Option	Action
	The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important:** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. • **Static** The wizard prompts you to enter the temporary IP address and network settings. • **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment.

13. On the Ready to complete stage 1 page, review the deployment settings for the target vCenter Server appliance and click **Finish** to start the OVA deployment process.
14. Wait for the OVA deployment process to finish and click **Continue** to proceed with stage 2 of the migration process to transfer the data from the source vCenter Server and start the services of the target appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface of the newly deployed target vCenter Server appliance to transfer the data from the source vCenter Server and set up the services.

The newly deployed target vCenter Server appliance version 7.0 is running on the target server but is not yet configured.

Important: The data from the source vCenter Server is not yet transferred and the services of the target appliance are not started.

Set Up the Target vCenter Server Appliance

When the OVA deployment completes, you are redirected to stage 2 of the migration process to transfer the data from the source vCenter Server and start the services of the newly deployed vCenter Server appliance version 7.0.

Your window of downtime does not begin until you begin to set up the target appliance. You cannot cancel or interrupt the process until it completes with the shut down of the source deployment. Your window of downtime ends when the target appliance starts.

1. Review the introduction to stage 2 of the migration process and click **Next**.
2. On the Select source vCenter Server page, enter the vCenter Single Sign-On administrator password and the root password of the source vCenter Server, enter the password of the user with administrative privileges on the vCenter Server instance, and click **Next**.
3. Optional: Accept the warning message, if any, by clicking **Yes**.
4. If your source Windows machine is connected to an Active Directory domain, enter the credentials for an administrator domain user with permission to add the target machine to the Active Directory domain, and click **Next**.

   Note: The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.
5. Review the VMware Customer Experience Improvement Program (CEIP) page and choose if you want to join the program.

   For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.
6. On the ready to complete page, review the migration settings, accept the backup acknowledgment, and click **Finish**.
7. Click **OK** to confirm the shutdown of the source vCenter Server.
8. Wait for the data transfer and setup process to finish and click **OK** to go to the vCenter Server Getting Started page.

The source vCenter Server instance is migrated from Windows to a vCenter Server appliance. The source vCenter Server instance is powered off and the new target appliance starts.

Verify that your migration to an appliance was successful. For verification steps, see Verify Your vCenter Server Upgrade or Migration Is Successful. For post-migration steps, see After Upgrading or Migrating vCenter Server.

GUI Migration of vCenter Server with an External Platform Services Controller to an Appliance

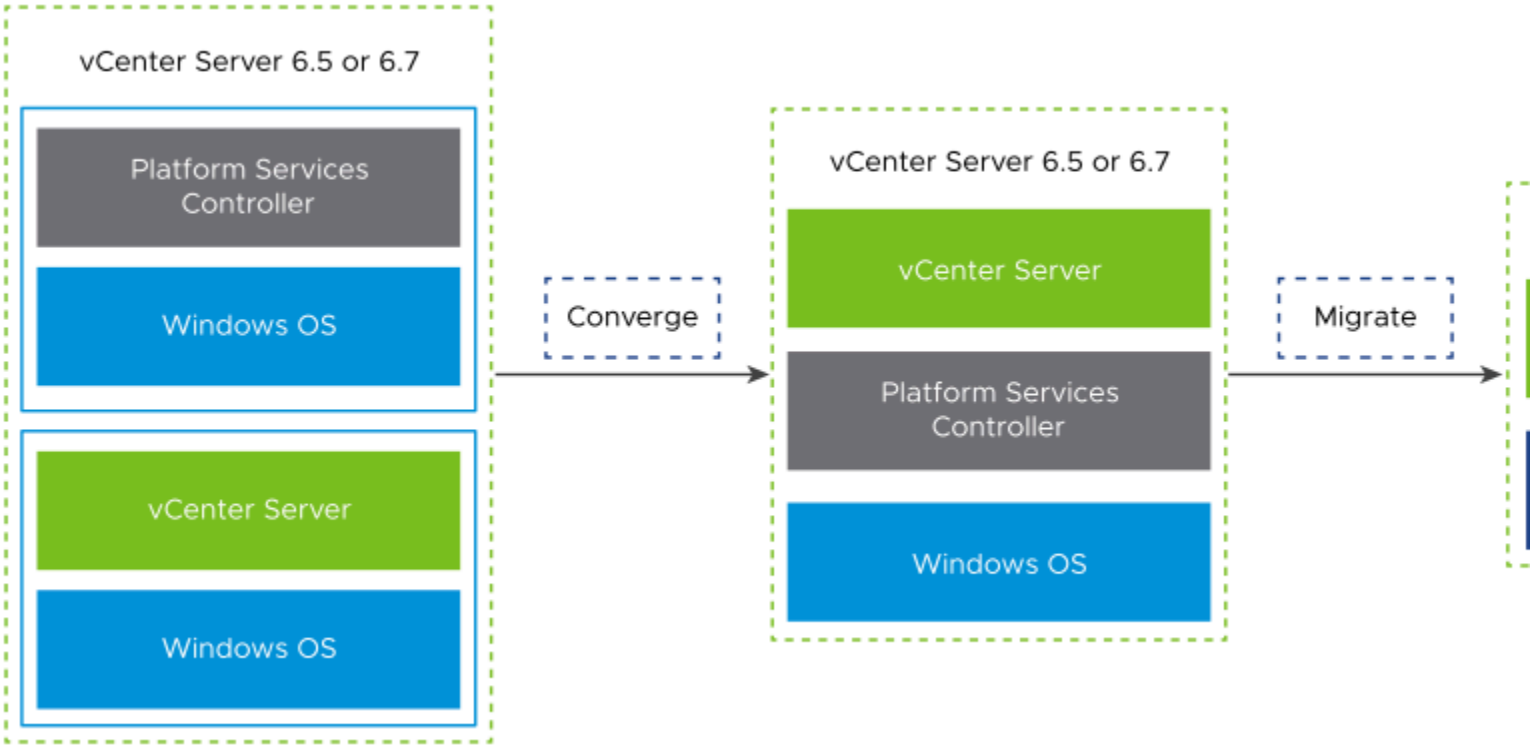
You can use the GUI to migrate vCenter Server with an external Platform Services Controller to a vCenter Server appliance.

Before migrating a vCenter Server deployment with an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the migration. See Knowledge Base article KB 68137.

If you use Update Manager in the deployment on Windows that you migrate, and Update Manager runs on a separate machine from any other of the components, take an extra step to migrate Update Manager to an appliance.

1. If your deployment on Windows uses an external Update Manager, run Migration Assistant on the Update Manager machine to start the migration of the Update Manager server and database to the Update Manager appliance.
2. Migrate the vCenter Server instance from Windows to a vCenter Server appliance.
3. Verify the newly migrated vCenter Server appliance.
4. Decommision the Platform Services Controller.

Figure 40: vCenter Server 6.5 or 6.7 with External Platform Services Controller Before and After Migration



GUI tasks for migrating an external Platform Services Controller instance from Windows to an appliance.

1. Download and Mount the vCenter Server Installer ISO file on a network virtual machine or physical server from which you want to perform the migration.
2. Download and Run VMware Migration Assistant on the Source Windows Machine.
   Note: If you are migrating a system that uses an external instance of Update Manager that runs on a separate Windows machine, first run Migration Assistant on the Update Manager machine.
3. Assemble the Required Information for Migrating vCenter Server from Windows to an Appliance for each Platform Services Controller or vCenter Server instance.
4. Deploy the OVA File for the Target vCenter Server Appliance
5. Set Up the Target vCenter Server Appliance

Important: The user name you use to log in to the physical machine from which you want to run the GUI installer, the path to the vCenter Server appliance installer, and values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

For each node to be migrated, the installer:

- Deploys a new target appliance.
- Exports the required files from the source Platform Services Controller or vCenter Server instance.
- Copies the required files to the target appliance for migration.
- Runs the migration process on the target appliance as indicated in the Summary.
- Imports and updates the files and settings of the source Platform Services Controller or vCenter Server instance to the new vCenter Server appliance.

Deploy the OVA File for the Target vCenter Server Appliance

To start the migration process, you use the GUI installer to deploy the OVA file that is included in the installer ISO file as the target vCenter Server appliance.

- See Prerequisites for Migrating vCenter Server

1. In the vCenter Server installer, navigate to the `vcsa-ui-installer` directory, go to the subdirectory for your operating system, and run the installer executable file.
   - For Windows OS, go to the `win32` subdirectory, and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory, and run the `Installer.app` file.
2. On the Home page, click **Migrate**.
3. Review the Introduction page to understand the migration process and click **Next**.
4. Read and accept the license agreement, and click **Next**.
5. Connect to the target server to which you want to migrate the source vCenter Server.

Option	Steps
You can connect to an ESXi host on which to deploy the target appliance.	1. Enter the FQDN or IP address of the ESXi host. 2. Enter the HTTPS port of the ESXi host. 3. Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**.
You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the target appliance.	1. Enter the FQDN or IP address of the vCenter Server instance. 2. Enter the HTTPS port of the vCenter Server instance. 3. Enter the user name and password of a vCenter Single Sign-On user with administrative privileges on the vCenter Server instance, for example, the administrator@*`your_domain_name`* user. 4. Click **Next**. 5. Accept the certificate warning, if any, by clicking **Yes**. 6. Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next** **Note:** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode. 7. Select the ESXi host or DRS cluster on which you want to deploy the new appliance, and click **Next**.

6. Optional: Review the warning message and try to resolve the warnings, if any, and click **Yes**.
7. On the Set up target appliance VM page, enter a name for the target vCenter Server Appliance, set the password for the root user, and click **Next**.

   The password must contain at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sigh (@), or brackets (()).

   Important: The local operating system password is not migrated to the target appliance.

8. On the Connect to source page, enter the details for the source vCenter Server instance, and click **Next**.
   a) Enter the IP address or FQDN.
   b) Enter the user name and password of a user who has administrative privileges on the vCenter Server instance, for example, the administrator@*your_domain_name* user.
   c) Enter the Migration Assistant Port you received in the Migration Assistant instructions.
9. On the Connect to source instance page, enter the details for the source Windows installation that you want to migrate.

Option	Action
vCenter Server IP Address/FQDN	Enter the IP address or FQDN of the vCenter Server Appliance that you want to upgrade.
vCenter Single Sign-On administrator user name	Enter the vCenter Single Sign-On administrator user name.
vCenter Single Sign-On administrator password	Enter the password of the vCenter Single Sign-On administrator.
vCenter Server HTTPS Port	Optionally, change the default vCenter Server HTTPS port number. The default value is 443.

10. Optional: Accept the warning message, if any, by clicking **Yes**.
11. Select the deployment size for the new vCenter Server Appliance for your vSphere inventory.

Deployment Size Option	Description
Tiny	Deploys an appliance with 2 vCPUs and 12 GB of memory. Suitable for environments with up to 10 hosts or 100 virtual machines
Small	Deploys an appliance with 4 CPUs and 19 GB of memory. Suitable for environments with up to 100 hosts or 1,000 virtual machines
Medium	Deploys an appliance with 8 CPUs and 28 GB of memory. Suitable for environments with up to 400 hosts or 4,000 virtual machines
Large	Deploys an appliance with 16 CPUs and 37 GB of memory. Suitable for environments with up to 1,000 hosts or 10,000 virtual machines
X-Large	Deploys an appliance with 24 CPUs and 56 GB of memory. Suitable for environments with up to 2,500 hosts or 45,000 virtual machines

Note: At the bottom of the deployment size table, a row shows the size information of the source machine. This size information is reported by the migration assistant and might help understand why you cannot select some deployment sizes.

12. Select the storage size for the new vCenter Server Appliance, and click **Next**.

Storage Size Option	Description for Tiny Deployment Size	Description for Small Deployment Size	Description for Medium Deployment Size	Description for Large Deployment Size	Description for X-Large Deployment Size
Default	Deploys an appliance with 315 GB of storage.	Deploys an appliance with 380 GB of storage.	Deploys an appliance with 600 GB of storage.	Deploys an appliance with 965 GB of storage.	Deploys an appliance with 1705 GB of storage.
Large	Deploys an appliance with 1390 GB of storage.	Deploys an appliance with 1435 GB of storage.	Deploys an appliance with 1600 GB of storage.	Deploys an appliance with 1665 GB of storage.	Deploys an appliance with 1805 GB of storage.
X-Large	Deploys an appliance with 3145 GB of storage.	Deploys an appliance with 3195GB of storage.	Deploys an appliance with 3360 GB of storage.	Deploys an appliance with 3425 GB of storage.	Deploys an appliance with 3565 GB of storage.

13. From the list of available datastores, select the location where all the virtual machine configuration files and virtual disks will be stored and, optionally, enable thin provisioning by selecting **Enable Thin Disk Mode**. NFS datastores are thin provisioned by default.
14. Configure the temporary network for communication between the source vCenter Server and the target vCenter Server appliance, and click **Next**.

Option	Action
Choose a network	Select the network to which to connect the new appliance temporarily. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are unsupported and are not displayed in the drop-down menu. **Important:** If you want to assign a temporary IPv4 address with DHCP allocation, you must select a network that is associated with a port group which accepts MAC address changes.
IP Address family	Select the version for the temporary IP address of the new appliance. Can be either IPv4 or IPv6.
Network type	Select the allocation method for the temporary IP address of the appliance. • **Static** The wizard prompts you to enter the temporary IP address and network settings. • **DHCP** A DHCP server is used to allocate the temporary IP address. Select this option only if a DHCP server is available in your environment.

15. On the Ready to complete stage 1 page, review the deployment settings for the target vCenter Server appliance and click **Finish** to start the OVA deployment process.
16. Wait for the OVA deployment to finish, and click **Continue** to proceed with stage 2 of the deployment process to set up and start the services of the newly deployed appliance.

    Note: If you exit the wizard by clicking **Close**, you must log in to the vCenter Server Management Interface to set up and start the services.

The newly deployed target vCenter Server appliance version 7.0 is running on the target server but is not yet configured.

Important: The data from the source vCenter Server is not yet transferred and the services of the target appliance are not started.

Set Up the Target vCenter Server Appliance

When the OVA deployment finishes, you are redirected to stage 2 of the migration process to transfer the data from the source vCenter Server and start the services of the newly deployed target vCenter Server appliance.

The period of time during which your system is unavailable does not begin until you start to set up the target appliance. You cannot cancel or interrupt the process until it finishes with the shutdown of the source deployment. The time your system is unavailable ends when the target appliance starts.

1. Review the introduction to stage 2 of the migration process and click **Next**.
2. On the Select source vCenter Server page, enter the vCenter Single Sign-On administrator password and the root password of the source vCenter Server, enter the password of the user with administrative privileges on the vCenter Server instance, and click **Next**.
3. Optional: Accept the warning message, if any, by clicking **Yes**.
4. If your source Windows machine is connected to an Active Directory domain, enter the credentials for an administrator domain user with permission to add the target machine to the Active Directory domain, and click **Next**.

   Note: The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.
5. Specify the replication topology for the vCenter Server. When converging vCenter Server instance with an external Platform Services Controller you must specify the replication topology.

   Convergence is the process of converting a vCenter Server instance with an external Platform Services Controller to a vCenter Server instance with those services embedded in the appliance.

   - This is the first vCenter Server in the topology that I want to converge.
   - This is a subsequent vCenter Server.

     If this is a subsequent vCenter Server, provide the IP address of its partner vCenter Server and its HTTPS port.
6. On the Select migration data page, choose the types of data that you want to transfer from the source vCenter Server to the target appliance.

   The large amount of data requires more time to be transferred to the new appliance.
7. On the ready to complete page, review the migration settings, accept the backup acknowledgment, and click **Finish**.
8. Click **OK** to confirm the shutdown of the source vCenter Server.
9. Wait for the data transfer and setup process to finish. Click **OK** to go to the vCenter Server Getting Started page.

vCenter Server is migrated from Windows to a newly deployed target vCenter Server appliance. The source vCenter Server is powered off and the target appliance starts.

- Verify Your vCenter Server Upgrade or Migration Is Successful.
- Upgrade all vCenter Server instances in the vCenter Single Sign-On domain.
- After converging a vCenter Server with an external Platform Services Controller node to a vCenter Server appliance, you must decommission the original external Platform Services Controller. Decommissioning a Platform Services Controller shuts it down and removes it from the single sign-on domain. See Decommission the Platform Services Controller.
- For post-migration steps, see After Upgrading or Migrating vCenter Server.
- You can configure high availability for the vCenter Server appliance. For information about providing vCenter Server appliance high availability, see *vSphere Availability*.

CLI Migration of a vCenter Server Installation from Windows to an Appliance

You can use the CLI installer to automatically migrate a vCenter Server or Platform Services Controller from Windows to an appliance.

The installer ISO file contains example templates of JSON files that contain the minimum configuration parameters required for migrating a vCenter Server or Platform Services Controller instance from Windows to an appliance. The example templates are located in the `vcsa-cli-installer/templates/migrate` directory.

Note: Before migrating a vCenter Server deployment with an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the migration. See Knowledge Base article KB 68137.

CLI tasks for migrating your vCenter Server installation from Windows to an appliance:

1. Download and Mount the vCenter Server Installer.
2. Download and Run VMware Migration Assistant on the Source Windows Machine.
3. Prepare JSON Configuration Files for CLI Migration.
4. Run the precheck before performing the migration.
5. Perform a CLI Migration of vCenter Server from Windows to an Appliance.

You can run the CLI installer multiple times with different JSON files to perform multiple CLI migrations, or you can run the CLI migrations concurrently in a batch mode.

Important: The user name that you use to log in to the machine from which you want to run the CLI installer, the path to the vCenter Server appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

Prepare JSON Configuration Files for CLI Migration

When you use the CLI to migrate a source vCenter Server installation to a target vCenter Server Appliance, you must prepare a JSON template with the configuration values for the new appliance.

Verify your environment meets the requirements for migration. See System Requirements for Migrating vCenter Server Deployments to Appliance Deployments,

Prepare your environment for migration. See Preparing for Migration.

You can migrate vCenter Server or Platform Services Controller instances from Windows to a vCenter Server Appliance by setting values to the configuration parameters in the templates that are available in the installer ISO file. The configuration parameters that are not included in the templates are set to their default values. You can add configuration parameters in the templates to set their values for your migration specification.

The `vcsa-cli-installer/templates/migrate` directory contains example migration templates for CLI migration of vCenter Server 6.5 and vCenter Server 6.7 to an appliance.

For a complete list of the configuration parameters and their descriptions, navigate to the installer subdirectory for your operating system and run the `vcsa-deploy migrate --template-help` command.

Important: The user name that you use to log in to the machine from which you want to run the CLI installer, the path to the vCenter Server Appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To perform the batch migration, place the JSON templates defining your deployment in a single directory. When invoked, the CLI installer migrates your existing deployment to the new vCenter Server version using the topology defined in the JSON templates.

1. Open the `migrate` subfolder in the `vcsa-cli-installer/templates` directory.
2. Copy the migration template from the `migrate` subfolder to your workspace.
   - For vCenter Server 6.5, use the `migrate/winvc6.5/` folder.
   - For vCenter Server 6.7, use the `migrate/winvc6.7/` folder.
3. Open the template file for your use case in a text editor.

   To ensure the correct syntax of your JSON configuration file, use a JSON editor.
4. Fill in values for the required configuration parameters and, optionally, enter additional parameters and their values.

   Important: To set a value that contains the backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"C:\\vmware\\vcsa"` sets the path `C:\vmware\vcsa`.

   The boolean values must contain only lowercase characters. Can be either `true` or `false` . For example, `"ssh_enable":false`
5. Save in UTF-8 format and close the file.

Your file is ready to use for migration.

You can create and save as many templates as are needed for your specific environment. When your template is ready, run the pre-check before using it to run the migration. See Run a Pre-Check Before a CLI Migration to vCenter Server Appliance.

JSON Templates for CLI Migration of vCenter Server for Windows

The vCenter Server installer contains JSON templates that are located in the `vcsa-cli-installer/templates` directory. In the `migrate` subfolder, you can find the JSON templates with the minimum configuration parameters for all migration types.

Table 80: Migration JSON Templates Included in the vCenter Server Installer

Location	Template	Description
`vcsa-cli-installer\templates\migrate\vcsa\6.5`	`embedded_win_vc_to_embedded_vCSA_on_ESXi.json`	Contains the minimum configuration parameters required to migrate vCenter Server 6.5 on Windows with an embedded Platform Services Controller, to a vCenter Server appliance 7.0 on an ESXi host.

Location	Template	Description
	embedded_win_vc_to_embedded_vCSA_on_VC.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.5 on Windows with an embedded Platform Services Controller to a vCenter Server appliance 7.0 on a vCenter Server instance.
	win_vc_to_vCSA_on_ESXi.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.5 on Windows with an external Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.
	win_vc_to_vCSA_on_VC.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.5 on Windows with an external Platform Services Controller to vCenter Server appliance 7.0 on a vCenter Server instance.
vcsa-cli-installer\templates\migrate\vcsa\6.7	embedded_win_vc_to_embedded_vCSA_on_ESXi.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.7 on Windows with an embedded Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.
	embedded_win_vc_to_embedded_vCSA_on_VC.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.7 on Windows with an embedded Platform Services Controller to vCenter Server Appliance7.0 on a vCenter Server instance.
	win_vc_to_vCSA_on_ESXi.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.7 on Windows with an external Platform Services Controller to vCenter Server appliance 7.0 on an ESXi host.
	win_vc_to_vCSA_on_VC.json.json	Contains the minimum configuration parameters required to migrate vCenter Server 6.7 on Windows with an external Platform Services Controller to vCenter Server appliance 7.0 on a vCenter Server instance.

About Migrating a vCenter Server for Windows with an External Platform Services Controller Using the CLI

When migrating a vCenter Server for Windows that uses an external Platform Services Controller, it is converted to a vCenter Server instance with those services embedded in the appliance. For this reason, you must specify replication partner parameters in the JSON migration templates.

When migrating a vCenter Server for Windows that uses an external Platform Services Controller, you must specify replication partner parameters in the JSON migrate template. These parameters indicate if the migration is for one of the following vCenter Server and Platform Services Controller migration scenarios.

- A single vCenter Server and a single Platform Services Controller instance within an SSO domain.

- The first vCenter Server and Platform Services Controller instance within an SSO domain containing more than one vCenter Server.
- Replicating vCenter Server and Platform Services Controller instances within an SSO domain, which you must point to an existing vCenter Server 7.0 instance as the replication partner.

Important: Before migrating a vCenter Server deployment using an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the migration. For more information, see Removal of Platform Services Controller.

Deployments using an external Platform Services Controller are often called an `MxN`deployment, where `M` represents the vCenter Server, and `N` represents the external Platform Services Controller. When representing multiple instances of vCenter Server and Platform Services Controller in a domain, this is expressed as `MnxNn`, where *n* is the number of instances. For example, `M2xN2` indicates two vCenter Server instances and two Platform Services Controller instances within the same domain. When migrating such a deployment, you first migrate one instance to version 7.0, and then migrate the second instance to 7.0, specifying the first of the two instances as the replicating partner.

The replication parameters in the JSON migration template are located in the `sso` section of the template, and are `first_instance` and `replication_partner_hostname` .

Parameter Name	Description
`first_instance`	The `first_instance` parameter identifies the vCenter Server as either the first instance in your vCenter Server SSO domain, or as a replicating partner. If it is the first vCenter Server instance, set `first_instance` to `true` For additional instances of vCenter Server in the same SSO domain, set `first_instance` to `false` .
`replication_partner_hostname` *	If you set `first_instance` to `false` , you must specify the FQDN or IP address of a vCenter Server that has already been migrated to version 7.0, and whose external PSC has been converged into the vCenter Server appliance.

When you perform the CLI migration of a single vCenter Server for Windows instance that uses an external Platform Services Controller, the process is as follows:

1. Migrate the vCenter Server in your topology using the `win_vc_to_vCSA_on_ESXi.json` template when migrating on ESXi, or the `win_vc_to_vCSA_on_VC.json` template when migrating on a vCenter Server deployment.
2. For a deployment topology consisting of a single vCenter Server and a Platform Services Controller (an `M1xN1` deployment), edit the `sso` section of the template such that the `first_instance` parameter is set to `true` , and remove the `replication_partner_hostname` parameter.

   ```
   "sso": {
   "__comments": [ This is the first instance (M1) vCenter Server management node, with "first_instance" set
    to "true" and "replication_partner_hostname" removed.
   ],
   "first_instance": true
   }
   ```

3. Specify the remaining configuration parameters in the JSON template, and migrate vCenter Server to version 7.0 using the CLI. See Perform a CLI Migration of vCenter Server from Windows to an Appliance.
4. After successfully migrating vCenter Server, decommission the Platform Services Controller. See Decommission the Platform Services Controller.

   Important: Decommission the Platform Services Controller instances only after migrating and converging all vCenter Server instances in your topology.

For a deployment consisting of two or more vCenter Server and Platform Services Controller instances (an M2xN2 deployment), you first migrate the M1vCenter Server instance to version 7.0, and then migrate the second, replicating vCenter Server instance.

1. Migrate the vCenter Server in your topology using the win_vc_to_vCSA_on_ESXi.json template when migrating on ESXi, or the win_vc_to_vCSA_on_VC.json template when migrating on a vCenter Server deployment.
2. For the first vCenter Server instance (M1), edit the sso section of the template such that the first_instance parameter is set to true , and remove the replication_partner_hostname parameter.

```
"sso": {
"__comments": [ This is the first instance (M1) vCenter Server management node, with "first_instance" set
 to "true" and "replication_partner_hostname" removed.
],
"first_instance": true
}
```

3. For the remaining vCenter Server instance (M2), edit the sso section of the template such that the first_instance parameter is set to false , and provide the FQDN or IP address of the vCenter Server instance to which you want to replicate the second node. The replication partner is the first vCenter Server instance (M1) you migrated to version 7.0, which has been converged with its Platform Services Controller instance.

```
"sso": {
"__comments": [ This is the second instance (M2) vCenter Server management node, with "first_instance" set
 to "false" and "replication_partner_hostname" set to the hostname of the replication partner.],
"first_instance": false,
"replication_partner_hostname": "FQDN_or_IP_address"
```

4. Specify the remaining configuration parameters in the JSON templates, and migrate vCenter Server to version 7.0 using the CLI. See Perform a CLI Migration of vCenter Server from Windows to an Appliance.
5. After successfully migrating all vCenter Server instances in the topology, decommission the Platform Services Controller instances. See Decommission the Platform Services Controller.

   Important: Decommission the Platform Services Controller instances only after migrating and converging all vCenter Server instances in your topology.

Migration Configuration Parameters

When using the CLI installer to migrate your vCenter Server installation to an appliance, you must provide the parameters with values for your migration specification.

The table lists the configuration parameters that you use to provide input data for the source vCenter Server.

Important: The path to the vCenter Server appliance installer, the path to your JSON configuration file, and the string values in your JSON configuration file, including passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are not supported.

To set a value that contains the backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, "password":"my\"password" sets the password my"password, "image":"C:\\vmware\\vcsa" sets the path C:\vmware\vcsa.

The boolean values must contain only lowercase characters. Can be either true or false . For example, "ssh_enable":false .

Sections and Subsections of Configuration Parameters in the JSON Migration Templates

The configuration parameters in the JSON migration templates are organized in sections and subsections.

Table 81: Sections and Subsections of Configuration Parameters in the JSON Migration Templates

Section	Subsection	Description
`new_vcsa` - describes the target appliance that you want to migrate to	`esxi`	Use only if you want to deploy the appliance directly on an ESXi host. Contains the configuration parameters that describe the target ESXi host. **Note:** You must fill in either the `esxi` or the `vc` subsection.
	`vc`	Use only if you want to deploy the appliance on the inventory of a vCenter Server instance. Contains the configuration parameters that describe the target ESXi host or DRS cluster from the vCenter Server inventory. **Note:** You must fill in either the `vc` or the `esxi` subsection.
	`appliance`	Contains the configuration parameters that describe the appliance.
	`os`	Contains the configuration parameters that describe the operating system settings for the appliance.
	`ovftool_arguments`	Optional subsection for adding arbitrary arguments and their values to the OVF Tool command that the installer generates. **Important:** The vCenter Server appliance installer does not validate the configuration parameters in the `ovftool_arguments` subsection. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
	`temporary_network`	Contains the configuration parameters that describe the temporary network for migrating the data from the source to the new target appliance.
	`user-options`	Use only when the source is a vCenter Server instance. Contains the configuration parameters that let you control aspects of the migration process for particular components.
`source_vc` - describes the source vCenter Server, vCenter Single Sign-On, or Platform Services Controller	`vc_win`	Contains the configuration parameters that describe the source Windows installation of vCenter Server or Platform Services Controller
	`run_migration_assistant`	Use only if the source Windows installation is running as a virtual machine and you want to automate the invocation of Migration Assistant. For a source Windows installation running on a physical machine, or if you are running Migration Assistant manually on the source Windows machine, copy and paste the thumbprint value from the Migration Assistant console output on the source machine to the `migration_ssl_thumbprint` key in the `vc_win` subsection, and remove the `run_migration_assistant` section.
`ceip` - describes joining the VMware Customer Experience Improvement Program (CEIP)	`settings`	Contains only the `ceip_enabled` configuration parameter to join or not to join the VMware Customer Experience Improvement Program (CEIP). Required only if you are deploying a vCenter Server appliance. **Note:** If set to `true` , you must run the CLI deployment command with the `--acknowledge-ceip` argument. For information about the CEIP, see the Configuring Customer Experience Improvement Program section in *vCenter Server and Host Management*.

Configuration Parameters in the `new_vcsa` Section

Table 82: Configuration Parameters in the `new_vcsa` Section, `esxi` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target ESXi host on which you want to deploy the appliance.
`username`	string	A user name with administrative privileges on the target ESXi host, for example, root.
`password`	string	The password of the user with administrative privileges on the target ESXi host.
`deployment_network`	string	The name of the network to which to connect the appliance. **Note:** The network must be accessible from the target ESXi host. Ignored if the target ESXi host has only one network.
`datastore`	string	The name of the datastore that you want to store all virtual machine configuration files and virtual disks of the appliance. **Note:** The datastore must be accessible from the ESXi host. The datastore must have enough free space.
`port`	integer	The port number of the ESXi host. The default port is 443.

`ssl_certificate_verification`	string	The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI stops the upgrade unless you specify one of the following SSL certificate configuration options.
		Specify the Secure Hash Algorithm 1 (SHA-1) certificate thumbprint. A certificate thumbprint is a hexadecimal string that uniquely identifies a certificate. The thumbprint is calculated from the content of the certificate using a thumbprint algorithm.
		`"thumbprint": "certificate SHA-1 thumbprint"`
		Set `verification_mode` to `NONE` .
		`"verification_mode": "NONE"`
		If you are connecting to a server with a self-signed certificate, and fail to either specify the SHA-1 certificate thumbprint, or set the verification mode to `NONE` , the CLI will display the server's self-signed certificate's thumbprint, and prompt you to accept or reject the certificate thumbprint.
		You can also specify that the CLI ignore the self-signed using the `vcsa-deploy upgrade` command parameter `--no-ssl-certificate-validation` . See Syntax of the CLI Migrate Command .

Table 83: Configuration Parameters in the `new_vcsa` Section, `vc` Subsection

Name	Type	Description
`hostname`	string	The IP address or FQDN of the target vCenter Server instance on which you want to deploy the appliance.
`username`	string	vCenter Single Sign-On administrator user name on the target vCenter Server instance, for example, administrator@vsphere.local.
`password`	string	The password of the vCenter Single Sign-On administrator user on the target vCenter Server instance.
`deployment_network`	string	The name of the network to which to connect the appliance. **Note:** The network must be accessible from the target ESXi host or DRS cluster on which you want to deploy the appliance. Ignored if the target ESXi host or DRS cluster has only one network.

Name	Type	Description

`datacenter`	string or array	The vCenter Server data center that contains the target ESXi host or DRS cluster on which you want to deploy the appliance.
		If the datacenter is located in a folder or a structure of folders, the value must be either a comma-separated list of strings or a comma-separated list as a single string. For example,
		`["parent_folder", "child_folder", "datacenter_name"]`
		or
		`"parent_folder, child_folder, datacenter_name"`
		If there is no folder path on the data center, then use only the datacenter name. For example,
		`["datacenter_name"]`
		or
		`"datacenter_name"`
		Note: The value is case-sensitive.

`datastore`	string	The name of the datastore that you want to store all virtual machine configuration files and virtual disks of the appliance. **Note:** The datastore must be accessible from the target ESXi host or DRS cluster. The datastore must have at least 25 GB of free space.
`port`	integer	The port number of the vCenter Server. The default port is 443.

`target`	string or array	The target cluster, ESXi host, or resource pool on which you want to deploy the new appliance. This is the target you specified with the `datacenter` parameter. This path must end with a cluster name, ESXi hostname, or resource pool name.
		Important: You must provide the name that is displayed in the vCenter Server inventory. For example, if the name of the target ESXi host is an IP address in the vCenter Server inventory, you cannot provide an FQDN.
		Note: All values are case-sensitive.
		If you want the deployed appliance to be listed in a different location within the data center's hierarchy, use the `vm_folder` parameter described later in this section.
		If the target cluster, ESXi host, or resource pool is located in a folder or a structure of folders, the value must be a comma-separated list of strings or a comma-separated list as a single string. For example,
		`["parent_folder", "child_folder", "esxi-host.domain.com"]`
		or
		`"parent_folder, child_folder, esxi-host.domain.com"`
		If the target ESXi host is part of a cluster, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["cluster_name", "esxi-host.domain.com"]`
		or
		`"cluster_name, esxi-host.domain.com"`
		If you are deploying to a resource pool, include the label `Resources` before the resource pool name. For example:
		`["cluster_name", "Resources", "resource_pool_name"]`
		Note: Pre-checks verify only the memory of the resource pool.

`vm_folder`	string	Optional. The name of the virtual machine (VM) folder to which to add the appliance.

Table 84: Configuration Parameters in the `new_vcsa` Section, `appliance` Subsection

Name	Type	Description
`thin_disk_mode`	Boolean	Set to `true` to deploy the appliance with thin virtual disks.
`deployment_option`	string	The size of the appliance. • Set to `tiny` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the default storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 300 GB of storage. • Set to `tiny-lstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 825 GB of storage. • Set to `tiny-xlstorage` if you want to deploy a vCenter Server appliance for up to 10 hosts and 100 virtual machines with the x-large storage size. Deploys an appliance with 2 CPUs, 10 GB of memory, and 1700 GB of storage. • Set to `small` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the default storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 340 GB of storage. • Set to `small-lstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 870 GB of storage. • Set to `small-xlstorage` if you want to deploy a vCenter Server appliance for up to 100 hosts and 1,000 virtual machines with the x-large storage size. Deploys an appliance with 4 CPUs, 16 GB of memory, and 1750 GB of storage. • Set to `medium` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the default storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 525 GB of storage. • Set to `medium-lstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1025 GB of storage. • Set to `medium-xlstorage` if you want to deploy a vCenter Server appliance for up to 400 hosts and 4,000 virtual machines with the x-large storage size. Deploys an appliance with 8 CPUs, 24 GB of memory, and 1905 GB of storage. • Set to `large` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the default storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 740 GB of storage. • Set to `large-lstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1090 GB of storage. • Set to `large-xlstorage` if you want to deploy a vCenter Server appliance for up to 1,000 hosts and 10,000 virtual machines with the x-large storage size. Deploys an appliance with 16 CPUs, 32 GB of memory, and 1970 GB of storage. • Set to `xlarge` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the default storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1180 GB of storage. • Set to `xlarge-lstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 1230 GB of storage. • Set to `xlarge-xlstorage` if you want to deploy a vCenter Server appliance for up to 2,000 hosts and 35,000 virtual machines with the x-large storage size. Deploys an appliance with 24 CPUs, 48 GB of memory, and 2110 GB of storage.
`image`	string	Optional. A local file path or URL to the vCenter Server appliance installation package.

Name	Type	Description
		By default the installer uses the installation package that is included in the ISO file, in the `vcsa` folder.
`name`	string	The VM name for the appliance. Must contain only ASCII characters except a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
`ovftool_path`	string	Optional. A local file path to the OVF Tool executable file. By default the installer uses the OVF Tool instance that is included in the ISO file, in the `vcsa/ovftool` folder.

Table 85: Configuration Parameters in the `new_vcsa` Section, `os` Subsection

Name	Type	Description
`password`	string	The password for the root user of the appliance operating system. The password must contain between 8 and 20 characters, at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character, for example, a dollar sign ($), hash key (#), at sign (@), period (.), or exclamation mark (!). All characters must be lower ASCII characters without spaces.
`ssh_enable`	Boolean	Set to `true` to enable the SSH administrator login to the appliance.

Table 86: Configuration Parameters in the `new_vcsa` Section, `temporary_network` Subsection

Name	Type	Description
`ip_family`	string	IP version for the network of the appliance. Set to `ipv4` or `ipv6` .
`mode`	string	IP assignment for the network of the appliance. Set to `static` or `dhcp` .
`ip`	string	IP address for the appliance. Required only if you use a static assignment, that is, if you set the `mode` parameter to `static` . You must set an IPv4 or IPv6 address that corresponds to the network IP version, that is, to the value of the `ip_family` parameter. An IPv4 address must comply with the RFC 790 guidelines. An IPv6 address must comply with the RFC 2373 guidelines.

`dns_servers`	string or array	IP addresses of one or more DNS servers.
		To set more than one DNS server, use a comma-separated list of strings or a comma-separated list as a single string to provide the path. For example,
		`["x.y.z.a", "x.y.z.b"]`
		or
		`"x.y.z.a, x.y.z.b"`
		Required only if you use a static assignment, that is, if you set the `mode` parameter to `static` .

`prefix`	string	Network prefix length. Required only if you use assignment, that is, if you set the `mode` parameter to `static` . For IPv4 version, the value must be between `0` and `32` . For IPv6 version, the value must be between `0` and `128` .
`gateway`	string	IP address of the default gateway. For IPv6 version, the value can be `default` .

Table 87: Configuration Parameters in the `new_vcsa` Section, `user_options` Subsection

Name	Type	Description
`vcdb_migrateSet`	string	Select the types of data to migrate from the old appliance to the new appliance. Data is copied from the source vCenter Server to the target server. The original source of the data remains unchanged. • Set to `core` if you want to transfer only the configuration data. This provides the fastest data migration, keeping system downtime to a minimum. • Set to `core_events_tasks` if you want to transfer the configuration and historical data (events and tasks) immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Windows. • Set to `all` if you want to transfer the configuration, historical, and performance metrics data immediately. vCenter Server will not start until all data has been migrated from the source vCenter Server for Windows. This option transfers the largest amount of data, and requires more downtime than other data migration options. • Set to `transfer_events_tasks_after_upgrade` if you want to transfer the historical data (events and tasks) in the background after the upgrade finishes. During this time, vCenter Server performance might not be optimal. • Set to `transfer_stats_events_tasks_after_upgrade` if you want to transfer historical data and performance metrics data in the background after the upgrade finishes. During this time, vCenter Server performance might not be optimal. **Note:** To minimize the migration time and the amount of storage required for the new vCenter Server appliance, use the `core` value. For more information on the types of data you can transfer from your existing vCenter Server to the new, upgraded vCenter Server, see Transferring Data After Upgrade or Migration.

Table 88: Configuration Parameters in the `new_vcsa` Section, `sso` Subsection

Name	Type	Description
`first_instance`	string	Set `first_instance` to `true` if this is the first converge migration operation in your vCenter Server SSO domain, or if you do not want to set the replication partner for this node. If you want to set the replication partner for this node, set `first_instance` to `false` and provide the value of the `replication_partner_hostname` as the FQDN of a previously converged node which is currently in an embedded vCenter Server topology. For more information on specifying the `first_instance` and `replication_partner_hostname` parameters, see About Migrating a vCenter Server for Windows with an External Platform Services Controller Using the CLI.
`replication_partner_hostname`	string	Host name of the replication partner. Remove if it is the `first_instance`

Requirements for the Automatic Invocation of Migration Assistant

You use the `run_migration_assistant` subsection to automate the invocation of Migration Assistant. Automatic invocation works only if the source Windows installation is running as a virtual machine.

The user account that you specify in the `os_username` or `vum_os_username` parameters needs a privilege elevation to Administrator. For example:

- The built-in Windows Administrator account.

- A user account with a user name other than Administrator that is a member of the local Windows Administrators group.
- The Domain Administrator account with the user name Administrator that is a member of the local Windows Administrators group.
- The user name ID must be in the format *your_domain_name**user_ID* or *user_ID*@*your_domain_name*.

Restriction: Automatic invocation of Migration Assistant does not work with a Windows account that requires a privilege elevation to Administrator. Instead, run Migration Assistant manually on the source Windows machine. Copy and paste the thumbprint value from the Migration Assistant console output on the source machine to the `migration_ssl_thumbprint` key in the `vc_win` subsection, and remove the `run_migration_assistant` section.

Configuration Parameters in the `source_vc` Section

Table 89: Configuration Parameters in the `source_vc` Section, `vc_win` Subsection

Name	Type	Description
`hostname`	string	The host name or IP address of the source Windows installation of vCenter Server or Platform Services Controller that you want to migrate.
`username`	string	A vCenter Single Sign-On user name with administrative privileges for the vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance that you want to migrate.
`password`	string	The password of the vCenter Server or Platform Services Controller instance that you want to migrate.
`migration_port`	string	Migration Assistant port number shown in the Migration Assistant console. The default port is 9123.
`active_directory_domain`	string	The name of the Active Directory domain to which the source vCenter Server instance is joined.
`active_directory_username`	string	Administrator user name of the Active Directory domain to which the source vCenter Server instance is joined.
`active_directory_password`	string	Administrator password of the Active Directory domain to which the source vCenter Server instance is joined. **Note:** The installer verifies the entered credentials, but does not check the required privileges to add the target machine to the Active Directory domain. Verify that the user credentials have all the required permissions to add a machine to the Active Directory domain.
`migration_ssl_thumbprint`	string	The SSL thumbprint of Migration Assistant.

Table 90: Configuration Parameters in the `source_vc` Section, `run_migration_assistant` Subsection

Name	Type	Description
`esxi_hostname`	string	FQDN or IP address of ESXi on which the source vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance resides.
`esxi_username`	string	User name of a user with administrative privileges on the ESXi host.
`esxi_password`	string	The password of the ESXi host user. If omitted, you are prompted to enter the password at the command console during the template verification.
`esxi_port`	string	The port number of the ESXi host. The default port is 443.
`os_username`	string	Administrator user name for the source Windows machine.

Name	Type	Description
os_password	string	Administrator user password for the source Windows machine. If omitted, you are prompted to enter it at the command console during the template verification.
migration_ip	string	The IP address of the network adapter to be migrated.
migration_port	string	Migration Assistant port number shown in the Migration Assistant console. The default port is 9123.
export_dir	string	Directory to export source configuration and data.
sa_password	string	The IP address of the network vCenter Server service account user password. This option is only required if the vCenter Server service is running under a non-LocalSystem account. If omitted, you are prompted to enter it at the command console during the template verification.

Table 91: Configuration Parameters in the `source_vum` Section, `run_migration_assistant` Subsection

Name	Type	Description
esxi_hostname	string	FQDN or IP address of ESXi on which the source vCenter Server, vCenter Single Sign-On, or Platform Services Controller instance resides.
esxi_username	string	User name of a user with administrative privileges on the ESXi host.
esxi_password	string	The password of the ESXi host user. If omitted, you are prompted to enter the password at the command console during the template verification.
esxi_port	string	The port number of the ESXi host. The default port is 443.
vum_hostname	string	FQDN or IP address of ESXi on which the source Update Manager instance resides.
vum_os_username	string	Administrator user name for the source Windows machine.
vum_os_password	string	Administrator user password for the source Update Manager Windows machine. If omitted, you are prompted to enter it at the command console during the template verification.
migration_port	string	Migration Assistant port number shown in the Migration Assistant console. The default port is 9123.
export_dir	string	Directory to export source configuration and data.

Configuration Parameters in the `ceip` Section

Table 92: Configuration Parameters in the `ceip` Section, `settings` Subsection

Name	Type	Description
ceip_enabled	Boolean	Set to `true` to join the CEIP for this appliance.

Run a Pre-Check Before a CLI Migration to vCenter Server Appliance

You can run a pre-check to verify that the migration requirements are met and resolve any problems before migration of your vCenter Server deployment.

Prepare JSON Configuration Files for CLI Migration using the example templates and configuration parameters.

Before migrating your vCenter Server deployment to an appliance, you can run a pre-check to find out the disk space requirement, the estimated upgrade time, and the extensions registered with the vCenter Server appliance. Running pre-upgrade is an optional but highly recommended step when planning your upgrade.

1. Verify your template without deploying the appliance by entering the command: `vcsa-deploy migrate --verify-template-only` *`path_to_json_file`*.
2. Run `CLI Migrate` using the `--precheck-only` option.

   You can adjust your migration plans using the disk space requirements and estimated migration time. If you receive an error, you can troubleshoot and resolve the problem before the actual migration.
3. After resolving any errors, run the `CLI Migrate` command using the `--verify-template-only` option again until all errors are resolved.

You are now prepared for an error-free CLI migration process.

Perform a CLI Migration of vCenter Server from Windows to an Appliance.

Perform a CLI Migration of vCenter Server from Windows to an Appliance

You can migrate vCenter Server to an appliance from a machine that is in your vSphere network.

- See Prerequisites for Migrating vCenter Server
- Create a snapshot of the deployment that you want to migrate as a precaution in case of failure during the migration process.
- Download the installer ISO file from the VMware website to a machine that is in your vSphere network. The installer ISO filename is VMware-VCSA-all-7.0.0-yyyyyy.iso, where yyyyyy is the build number. See Download and Mount the vCenter Server Installer.
- Prepare JSON Configuration Files for CLI Migration.
- Run a Pre-Check Before a CLI Migration to vCenter Server Appliance to identify problems and refine your migration plan.
- Review the optional arguments for running the migration. See Syntax of the CLI Migrate Command.

1. Navigate to the software CLI installer directory for your operating system.
   - If you are deploying the appliance from a machine with Windows OS, navigate to the `vcsa-cli-installer\win32` directory.
   - If you are deploying the appliance from a machine with Linux OS, navigate to the `vcsa-cli-installer/lin64` directory.
   - If you are deploying the appliance from a machine with Mac OS, navigate to the `vcsa-cli-installer/mac` directory.
2. Select the CLI installer: vcsa-deploy.exe.
3. Run the migration command.

   ```
   vcsa-deploy migrate --accept-eula optional_argumentspath_to_the_json_file
   ```

   The *`optional_arguments`* variable is a space-separated list of optional arguments to set additional configurations.

   For example, you can set the location of the log and other output files that the installer generates.

   ```
   vcsa-deploy migrate --accept-eula --log-dir=path_to_the_locationpath_to_the_json_file
   ```

The migration template is deployed. You can Verify Your vCenter Server Upgrade or Migration Is Successful.

Syntax of the CLI Migrate Command

You can use one or more command arguments to set the execution parameters of the migrate command.

You can add a space-separated list of arguments to the CLI upgrade command.

```
vcsa-deploy migrate list_of_argumentspath_to_the_json_file
```

The required `template` argument provides the path of a JSON file that describes the vCenter Server appliance deployment procedure. You can place multiple JASON files in a directory, and the CLI will migrate all of the deployments in batch mode. For more information on performing concurrent migrations, see Prepare JSON Configuration Files for CLI Migration.

Important: The string values, including the passwords, must contain only ASCII characters. Extended ASCII and non-ASCII characters are unsupported.

To set a value that contains the backslash (\) or quotation mark (") character, you must precede the character with the backslash (\) character. For example, `"password":"my\"password"` sets the password my"password, `"image":"C:\\vmware\\vcsa"` sets the path `C:\vmware\vcsa`.

The boolean values must contain only lowercase characters. Can be either `true` or `false` . For example, `"ssh.enable":false` .

Optional Argument	Description
`--accept-eula`	Accepts the end-user license agreement. Required for executing the deployment command.
`-h, --help`	Displays the help message for the command.
`--template-help`	Displays the help message for the configuration parameters in the JSON deployment file. You can use `vcsa-deploy [subcommand] --help` for a list of subcommand-specific arguments.
`-v, --verbose`	Adds debug information to the console output.
`-t, --terse`	Hides the console output. Displays only warning and error messages.
`--log-dir, LOG_DIR`	Specifies the location of the log and other output files that the installer generates.
`--skip-ovftool-verification`	Performs basic verification of the configuration parameters and deploys the vCenter Server appliance, but does not validate the OVF Tool parameters in the `ovftool_arguments` subsection of the JSON template. If you set arguments that the OVF Tool does not recognize, the deployment might fail.
`--no-ssl-certificate-verification`	Prohibits SSL verification of ESXi connections. The CLI verifies that a server's security certificate is signed by a Certificate Authority (CA), and establishes a secure connection. If the certificate is self-signed, the CLI will stop the upgrade unless you specify that the CLI ignore the self-signed certificate using the `--no-ssl-certificate-validation` command parameter. If you are connecting to a server with a self-signed certificate, and fail to specify that the CLI accept it, the CLI displays the server's self-signed certificate thumbprint, and prompts you to accept or reject the it.

Optional Argument	Description
	You can also specify that the CLI ignore self-signed certificates using the `ssl_certificate_verification` configuration parameter in the JSON template. See Upgrade Configuration Parameters for CLI Upgrade of vCenter Server Appliance . **Important:** Avoid using this option as it may cause problems during or after upgrade due to an un-validated identity of the target host.
`--operation-id`	Lets you provide an identifier to track the concurrent installation, migration, or upgrade of multiple vCenter Server instances. If do not provide an operation ID, the CLI generates a universally unique identifier (UUID) which you can use to identify the different instances of vCenter Server and their installation or upgrade status.
`--verify-template-only`	Performs basic template verification without installing Upgrade Runner, running prechecks, and upgrading or migrating the vCenter Server appliance.
`--precheck-only`	Installs Migration Assistant on the source vCenter Server virtual machine, and runs a complete set of prechecks without performing the migration.
`--acknowledge-ceip`	Confirms acknowledgement of your VMware Customer Experience Improvement Program (CEIP) participation. This argument is required if `ceip.enabled` is set to true in the upgrade template.

Exit Code	Description
0	Command ran successfully
1	Runtime error
2	Validation error
3	Template error

After Upgrading or Migrating vCenter Server

After you upgrade to vCenter Server, consider the post-upgrade options and requirements.

- Complete any component reconfigurations that might be required for changes during upgrade.
- Verify that you understand the authentication process and identify your identity sources.
- If you migrated vCenter Server on Windows to a target vCenter Server appliance and you use any local OS user names to log in to the vCenter Single Sign-On, you must recreate them and reassign permissions.
- If you performed an upgrade, upgrade any additional modules that are linked to this instance of vCenter Server, such as Update Manager. If you performed a migration from vCenter Server for Windows to a vCenter Server appliance, the Update Manager module is migrated as well into vSphere Lifecycle Manager.
- Optionally, upgrade or migrate the ESXi hosts in the vCenter Server inventory to the same version as the vCenter Server instance.

- If you use Update Manager in your vCenter Server deployment, and Update Manager and vCenter Server were running on separate machines prior the migration, consider to shut down or delete the Update Manager host machine after the migration is complete. Before disposing of the Update Manager host machine, take into account the following:
  - You might need the host machine for rolling back purposes of your upgraded or migrated environment.
  - You might have other software that runs on that machine.

Verify Your vCenter Server Upgrade or Migration Is Successful

You can verify the success of your vCenter Server upgrade or migration.

You must be logged into the upgraded or migrated vCenter Server instance. If you created a reference of required information based or a CLI template, you can use it to validate the upgrade or migration success.

1. Verify that the IP address is correct.
2. Verify that the Active Directory registration has not changed.
3. Verify the Network registration is correct.
4. Verify the Domain is correct.
5. Verify the certificates are valid.
6. Verify the inventory data is correctly migrated.
   a) Review the events history.
   b) Review the performance charts.
   c) Review the users, permissions, and roles.

If the postupgrade or postmigration configuration conforms to your required information or CLI template reference and expectations, the vCenter Server upgrade or migration is complete.

You can troubleshoot unexpected behavior by reviewing logs. You can also perform a rollback to the source configuration. See Roll Back a vCenter Server Upgrade or vCenter Server on Windows Migration

Log In to vCenter Server by Using the vSphere Client

You can use the vSphere Client to log in to vCenter Server and manage your vSphere inventory.

The vSphere Client is automatically installed as part of the vCenter Server appliance deployment. This way, the vSphere Client always points to the same vCenter Single Sign-On instance.

1. Open a Web browser and enter the URL for your vCenter Server instance:
   `https://vcenter_server_ip_address_or_fqdn`
   As an alternative, you can open a Web browser and enter the URL for the vSphere Client:
   `https://vcenter_server_ip_address_or_fqdn/ui`.
2. If a warning message about a potential security risk appears, select to continue to the website.

Browser	Action
Microsoft Edge	1. Click **Details**. 2. Under the additional message that appears, click **Go on to the webpage**.
Mozilla Firefox	1. Click **Advanced**. 2. Under the additional message that appears, click **Accept the Risk and Continue**.
Google Chrome	1. Click **Advanced**. 2. Under the additional message that appears, click **Proceed to *vcenter_server_ip_address_or_fqdn***.

3. On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.
4. If the warning message about a potential security risk appears again, repeat Step 2.
5. Enter the credentials of a user who has permissions on vCenter Server and click **Login**.

The vSphere Client connects to all the vCenter Server systems on which the specified user has permissions, and you can view and manage the vSphere inventory.

Decommission the Platform Services Controller

After you upgrade to vCenter Server appliance, can decommission external Platform Services Controller instances.

Make sure no vCenter Server instances are pointing to the Platform Services Controller before decommissioning.

Reconfigure any products deployed into the environment that use the Platform Services Controller to use the newly deployed vCenter Server appliance.

Make a backup of the Platform Services Controller before decommissioning to ensure no loss of data.

After converging an external Platform Services Controller node to a vCenter Server appliance, decommission the original external Platform Services Controller. Decommissioning a Platform Services Controller shuts it down and removes it from the single sign-on domain.

Decommission an External Platform Services Controller Appliance

Decommission and remove an external Platform Services Controller appliance from the vSphere inventory.

Make sure no vCenter Server instances are pointing to the Platform Services Controller before decommissioning.

Reconfigure any products deployed into the environment that use the Platform Services Controller to use the newly deployed vCenter Server appliance.

Make a backup of the Platform Services Controller before decommissioning to ensure no loss of data.

After converging an external Platform Services Controller node to a vCenter Server appliance, decommission the original external Platform Services Controller. Decommissioning a Platform Services Controller shuts it down and removes it from the single sign-on domain.

1. Stop the Platform Services Controller that you no longer need.
2. Log in as root to the appliance shell of one of the Platform Services Controller appliances within the domain.
3. Enable access to the Bash shell using the `shell.set --enabled true` command.
4. Start the Bash shell using the `shell` command, and log in.
5. Unregister the stopped Platform Services Controller appliance using the `cmsso-util unregister` command.

   Where, *`Platform_Services_Controller_System`* is the FQDN or IP address of the

   Platform Services Controller that you want to decommission. Run this command only on one of the Platform Services Controller replication partners, as the synchronization removes the entries from all other Platform Services Controller replication partners. Enter the `vCenter_Single_Sign_On_password` in quotes.

   Note: The `cmsso-util unregister` command restarts the services on the Platform Services Controller on which you are running the command. It can take several minutes for the command to finish.

   ```
   cmsso-util unregister --node-pnid Platform_Services_Controller_System --username administrator@your_do-
   main_name --passwd 'vCenter_Single_Sign_On_password'
   ```

6. Remove the Platform Services Controller appliance that you no longer need from the vSphere inventory.

You can delete the virtual machine for the decommissioned Platform Services Controller.

Ensure that any external solutions or products are registered with the new vCenter Server appliance.

Decommission an External Platform Server Controller for Windows

Decommission and remove an external Platform Services Controller for Windows from the vSphere inventory.

Make sure no vCenter Server instances are pointing to the Platform Services Controller before decommissioning.

Reconfigure any products deployed into the environment that use the Platform Services Controller to use the newly deployed vCenter Server appliance.

Make a backup of the Platform Services Controller before decommissioning to ensure no loss of data.

After converging an external Platform Services Controller node to a vCenter Server appliance, decommission the original external Platform Services Controller. Decommissioning a Platform Services Controller shuts it down and removes it from the single sign-on domain.

1. On the Windows computer running Platform Services Controller, click **Start** > **Run**, type `cmd`, and click **OK**.
   The Command Prompt opens.
2. Navigate to the directory `C:\Program Files\VMware\vCenter Server\bin\`
3. Unregister the stopped Platform Services Controller appliance using the `cmsso-util unregister` command.

   Where, *`Platform_Services_Controller_System`* is the FQDN or IP address of the Platform Services Controller that you want to decommission. Run this command only on one of the Platform Services Controller replication partners, as the synchronization removes the entries from all other Platform Services Controller replication partners. Enter the *`vCenter_Single_Sign_On_password`* in quotes.

   Note: The `cmsso-util unregister` command restarts the services on the Platform Services Controller on which you are running the command. It can take several minutes for the command to finish.

   ```
   cmsso-util unregister --node-pnid Platform_Services_Controller_System --username administrator@your_domain_name --passwd 'vCenter_Single_Sign_On_password'
   ```

4. Remove the Platform Services Controller appliance that you no longer need from the vSphere inventory.

You can delete the virtual machine for the decommissioned Platform Services Controller.

Ensure that any external solutions or products are registered with the new vCenter Server appliance.

Identity Sources for vCenter Server with vCenter Single Sign-On

You can use identity sources to attach one or more domains to vCenter Single Sign-On. A domain is a repository for users and groups that the vCenter Single Sign-On server can use for user authentication.

Note: At any time, only one default domain exists. If a user from a non-default domain logs in, that user must add the domain name to authenticate successfully. The domain name is in the form:

`DOMAIN\user`

The following identity sources are available.

- Active Directory over LDAP. vCenter Single Sign-On supports multiple Active Directory over LDAP identity sources.
- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources.

Note: A future update to Microsoft Windows will change the default behavior of Active Directory to require strong authentication and encryption. This change will impact how vCenter Server authenticates to Active Directory. If you use Active Directory as your identity source for vCenter Server, you must plan to enable LDAPS. For more information about this Microsoft security update, see https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 and https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Reregister Plug-In Solution in vCenter Server After Upgrade or Migration

You reregister a previously registered plug-in solution and any third-party client plug-in packages with vCenter Server after the SSL certificate has been refreshed following an upgrade or migration.

Consult the vendor documentation for any solution-based vCenter Server extensions and client plug-ins for instructions to re-register after a vCenter Server upgrade or migration.

If the procedure provided by your plug-in solution vendor fails to reregister the plug-in, you can use the following procedure to remove the plug-in registration, and then register it again with vCenter Server. For information on registering plug-ins, see the *vCenter Server and Host Management* documentation. For information on removing or disabling unwanted plug-ins from vCenter Server, see Knowledge Base article KB 102536.

1. In a Web browser, navigate to the Managed Object Browser of your vCenter Server.
   `https://vcenter_server_ip_address_or_fqdn/mob/?moid=ExtensionManager`
2. Log in with your vCenter Server credentials.
3. On the `ManagedObjectReference:ExtensionManager` page, under Methods, click **UnregisterExtension**.
4. On the `void UnregisterExtension` page, in the text box inside the Value column, enter the value for the `key` property of the `Extension` data object of your vSphere Client extension.
5. To unregister the extension click **Invoke Method**.

Go to the solution registration page and register the plug-in.

Verify that your extension is registered successfully with vCenter Server by using one of the following approaches.

- In the vSphere Client, go to Administration and under Solutions, select **Client Plug-Ins** and click **Check for New Plug-Ins**.
- Log out and log in again to the vSphere Client. The vSphere Client checks for new plug-ins for each new user session

Roll Back a vCenter Server Upgrade or vCenter Server on Windows Migration

You can roll back a vCenter Server upgrade or migration by reverting to the source appliance or vCenter Server on Windows.

You must have access to the source vCenter Server appliance or vCenter Server on Windows.

The rollback procedure applies in the following upgrade and migration contexts:

- vCenter Server appliance with an embedded Platform Services Controller .
- vCenter Server appliance with an external Platform Services Controller .

To revert a failed migration of vCenter Server, see Knowledge Base article KB 2146453.

Monitor and Manage Historical Data Migration

You can monitor and manage the background migration of historical data using the vCenter Server Management Interface.

- Verify that vCenter Server is successfully deployed and running.
- You must have selected to import historical data from the external database in use by the previous version of vCenter Server, to the embedded PostgreSQL database in vCenter Server7.0. See Transferring Data After Upgrade or Migration.

Using the vCenter Server Appliance Management Interface, you can perform the following data management tasks:

- Monitor the progress of the data migration.

- Pause the data migration.
- Cancel the data migration.

1. In a Web browser, go to the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.
2. Log in as root.

   The default root password is the password you set when deploying vCenter Server .
3. A status bar at the top of the vCenter Server Management Interface displays the percentage of data that has been copied from the source vCenter Server to the PostgreSQL database embedded in the target vCenter Server appliance.
4. To pause or cancel the data migration, click **Manage**.

Option	Description
Pause	During the data migration, vCenter Server performance might not be optimal. Pausing the migration lets vCenter Server run with better performance until such time that you can resume the process when it does not interfere with the needs of your business.
Resume	You can resume the data migration at a time that does not interfere with the business needs of your vCenter Server deployment.
Cancel	If you cancel the data import, the historical data will fail to import to the embedded PostgreSQL database. You cannot recover the data once you cancel the operation. If you cancel the import process, and want to import the historical data later, you must restart the upgrade or migration process from Stage 1 of the GUI installer.

When the data has been migrated, a success message displays in the vCenter Server Management Interface status bar.

Managing Software Updates, Upgrades, and Product Compatibility

You can view available vCenter Server updates and upgrades and produce interoperability reports about VMware products associated with vCenter Server. The reports help you plan vCenter Server updates and upgrades in your environment.

You can perform an interoperability check of VMware products within your environment against both source and target vCenter Server versions. You can also generate a pre-update report to ensure your environment meets the minimum software and hardware requirements for a successful upgrade of vCenter Server. You can plan vCenter Server updates and upgrades based on the information in the reports you generate.

Interoperability report for the current vCenter Server	Lists VMware products in your environment and their compatibility with the current, or source, version of vCenter Server.
Interoperability reports for target versions of vCenter Server	Lists the VMware products in your environment and their compatibility against the target version of vCenter Server to which you want to upgrade.
Pre-update reports	With the pre-update report, you can ensure that your system meets the minimum software and hardware requirements for a successful upgrade of vCenter Server. The report provides information about problems that might prevent the completion of a software upgrade, and actions you can take to remedy those problems.

Monitor Interoperability for the Current vCenter Server Version

You can view an interoperability report that lists products in your environment associated with the current vCenter Server version and their compatibility.

To use Update Planner, you must join the VMware Customer Experience Improvement Program (CEIP). For information about the CEIP, see the "Configuring Customer Experience Improvement Program" section in *vCenter Server and Host Management*.

The product interoperability report lists available products in your environment and their compatibility with the selected vCenter Server version.

1. In the vSphere Client navigate to a vCenter Server for which you want to view an interoperability report.
2. On the **Monitor** tab, click **Interoperability**.

   The Product Interoperability report lists all available products in your environment associated with the selected vCenter Server.
3. (Optional) If there are VMware products in your environment that go undetected, you can manually add them to the list of products to check and regenerate the interoperability report.
   a) Click **Add Product** in the Product Interoperability pane.
   b) Select the VMware product and version you want to include in the interoperability report.

      Repeat this step for each VMware product you want to add to the report.
   c) To add the selected products to the product inventory click **Done**.
   d) Regenerate the report and verify that the products you added are included in the report.
4. (Optional) Click **Export** in the Product Interoperability pane to export and save a copy of the report as a comma-separated values (CSV) file, which allows data to be saved in a tabular format.

- Using the information in the report, you can apply patches and updates to your vCenter Server environment. See Patching and Updating vCenter Server7.0 Deployments.
- You can generate a pre-upgrade report that lists actions that you must address to ensure a successful upgrade of vCenter Server in your environment. See Generate an Interoperability Report for Target vCenter Server Versions.

Generate an Interoperability Report for Target vCenter Server Versions

You can use Update Planner to perform pre-checks and generate reports that provide product interoperability information for recommended update and upgrade versions of vCenter Server.

To use Update Planner, you must join the VMware Customer Experience Improvement Program (CEIP). For information about the CEIP, see the "Configuring Customer Experience Improvement Program" section in *vCenter Server and Host Management*.

You can create a vCenter Server pre-update interoperability report to check the compatibility of VMware products in your environment againist a pending version of vCenter Server. Update Planner lists the products in your environment associated with the current vCenter Server version, and wheather or not those products are compatible with a suggested update version.

1. In the vSphere Client, select a vCenter Server for which you want to view an interoperability report.
2. On the **Updates** tab, click **Update Planner**
3. Select the target vCenter Server on which you want to run an interoperability check from the list of available updates. The list can contain minor updates and major upgrade versions of vCenter Server.
4. Click the **Generate Report** drop-down menu and select **Interoperability**.

   The Interoperability report displays in the bottom pane of the Pre-Update Checks panel.

5. (Optional) If there are VMware products in your environment that go undetected by Update Planner, you can manually add them to the list of products to check and regenerate the interoperability report.
   a) Click **Add Product** in the Product Interoperability pane.
   b) Select the VMware product and version you want to include in the interoperability report.
      Repeat this step for each VMware product you want to add to the report.
   c) To add the selected products to the Update Planner product inventory click **Done**.
   d) Regenerate the report and verify that the products you added are included in the report.
6. (Optional) Click **Export** in the Product Interoperability pane to save the report as a comma-separated values (CSV) file, which allows data to be saved in a tabular format.

- Using the information in the pre-upgrade report, you can apply patches and updates to your vCenter Server environment. See Patching and Updating vCenter Server7.0 Deployments.
- You can generate a pre-upgrade report that lists actions that you must address to ensure a successful upgrade of vCenter Server in your environment. See Generate an Interoperability Report for Target vCenter Server Versions.

Generate Pre-Update Reports

You can use Update Planner to run pre-checks and generate reports that provide pre-update information. You use this information to make sure that your system meets the minimum software and hardware requirements to ensure a successful upgrade of vCenter Server.

When you generate a pre-update report, Update Planner generates a list with actions that you must address to ensure a successful upgrade of vCenter Server in your environment. The report provides information about problems that might prevent the completion of a software upgrade or update.

1. In the vSphere Client, select a vCenter Server for which you want to view a pre-update report.
2. On the **Updates** tab, click **Update Planner**
3. Select the target vCenter Server on which you want to run a pre-upgrade check from the list of available servers in your environment.
4. Click the **Generate Report** drop-down menu and select **Pre-Update Checks**.
   The report displays in the bottom pane of the Pre-Update Checks panel.
5. (Optional) Click **Export** in the Pre-Update Checks pane to save the report as a comma-separated values (CSV) file, which allows data to be saved in a tabular format.
6. (Optional) Click **Open Appliance Management** to open the vCenter Server Management Interface, or **Download ISO** to download the selected ISO image with which to upgrade vCenter Server to the the selected target release.
   You use the vCenter Server Management Interface to perform administrative tasks such as monitoring vCenter Server, changing the host name and the network configuration, and applying patches and updates.

- Using the information in the pre-upgrade report, you can apply patches and updates to your vCenter Server environment. See Patching and Updating vCenter Server7.0 Deployments.
- You can generate an interoperability report that lists available VMware products in your environment, and the versions compatible with the vCenter Server version for which you are generating the report. See Generate an Interoperability Report for Target vCenter Server Versions.

Patching and Updating vCenter Server7.0 Deployments

You can update the vCenter Server with patches by using the `software-packages` utility available in the vCenter Server appliance shell.

Patching vCenter Server

VMware regularly releases patches for the vCenter Server. You can use the Appliance Management Interface or the appliance shell to apply patches to a vCenter Server.

VMware makes patches available on a monthly basis. These patches can only be applied in between major releases of vCenter Server. For example, patches released for the initial release of vCenter Server7.0, are not applicable to vCenter Server7.0 Update 1, as any patches previously made available will be included with the Update 1 release.

These patches can be for core product functionality, other packages in the vCenter Server such as Photon, or both.

Note: You must use only the patches provided by VMware to update the packages in your vCenter Server. Updating these packages through any other means may impact the product functionality.

VMware distributes the available patches in two forms, one for ISO-based and one for URL-based models of patching.

- You can download the patch ISO images from https://www.broadcom.com/support.
  VMware publishes a single type of ISO image that contains patches.

Download Filename	Description
`VMware-vCenter-Server-Appliance-`*`product_version-build_number`*`-patch-FP.iso`	Full product patch for the appliance, which contains the VMware software patches and the fixes related to security and third-party products (e.g. JRE and Photon OS components).

- You can configure the vCenter Server appliance to use a repository URL as a source of available patches.

Note:

The default online depot URLs are now unique for each customer. To update the default URLs of the online depot, see the following KB articles: KB 390098and KB 390121.

Patching vCenter Server Using the vCenter Server Management Interface

You can use the vCenter Server Management Interface to view the installed patches, check for new patches and install them, and configure automatic checks for available patches.

To perform ISO-based patching, you download an ISO image, attach the ISO image to the CD/DVD drive of the appliance, check for available patches in the ISO image, and install the patches.

To perform URL-based patching, you check for available patches in a repository URL and install the patches. The vCenter Server is preset with a default VMware repository URL for the build profile of the appliance. You can configure the appliance to use the default VMware repository URL or a custom repository URL, for example, a repository URL that you previously built on a local Web server running within your data center.

Log In to the vCenter Server Management Interface

Log in to the vCenter Server Management Interface to access the vCenter Server configuration settings.

Verify that the vCenter Server is successfully deployed and running.

Note: The login session expires if you leave the vCenter Server Management Interface idle for 10 minutes.

1. In a Web browser, go to the vCenter Server Management Interface, https://*`appliance-IP-address-or-FQDN`*:5480.
2. Log in as root.
   The default root password is the password that you set while deploying vCenter Server.

Check for and Stage Patches to the vCenter Server Appliance

Before you install available patches, you can stage the patches to the appliance. You can use the vCenter Server Management Interface to stage patches either from a local repository by attaching an ISO image to the appliance, or from a remote repository directly by using a repository URL.

- If you are staging patches from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance using the vSphere Client. See *vSphere Virtual Machine Administration*.
- If you are staging patches from a remote repository, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure URL-Based Patching.

During the process of staging, the vCenter Server Management Interface validates that a patch is a VMware patch, that the staging area has enough free space, and that the patches are not altered. Only new patches or patches for existing packages that can be upgraded are staged.

If a problem that prevents the successful staging of the patches occurs, vCenter Server suspends the staging process. Review the error messages, correct the problem, and, in many cases, you can resume staging the patches from the point at which vCenter Server encountered the problem.

1. Log into the vCenter Server Management Interface as root.

   The default root password is the password you set when deploying vCenter Server.

2. Click **Update**.

3. Click **Check Updates** and select a source.

Option	Description
Check URL	Scans the configured repository URL for available patches.
Check CDROM	Scans the ISO image that you attached to the CD/DVD drive of the appliance for available patches.

   In the Available Updates pane, you can view the details about the available patches in the source that you selected.

   Important: Some updates might require a reboot of the system. You can see information about these updates in the Available Updates pane.

4. You can run a pre-check of an update to verify that it is compatible with your current deployment.

5. Click the staging option you would like to use.

Option	Description
Stage	Stages the selected patches to the vCenter Server appliance for installation at a later time.
Stage and Install	Stages and installs the selected patches to the vCenter Server appliance. For more information on installing patches, see Install vCenter Server Patches.
Unstage	Unstages the selected patches.
Resume	If vCenter Server encounters a problem staging the patches, the vCenter Server Management Interface displays the **Resume** button. Correct the problem preventing the patches from staging, and click **Resume** to finish staging the patches. The staging process resumes from the point at which vCenter Server encountered the problem.

If you decided to stage the available patches for installation at a later time, you can now install. See Install vCenter Server Patches.

Configure the Repository for URL-Based Patching

For URL-based patching, by default the vCenter Server appliance is configured to use the default VMware repository URL that is preset for the build profile of the appliance. You can configure a custom repository URL as the current source of patches for your environment's requirements.

Log in to the vCenter Server Management Interface as root.

By default the current repository for URL-based patching is the default VMware repository URL.

If vCenter Server is not connected to the Internet or if your security policy requires it, you can build and configure a custom repository. The custom patching repository runs on a local Web server within your data center and replicates the data from the default repository. Optionally, you can set up an authentication policy for accessing the Web server that hosts the custom patching repository.

1. If you want to configure a custom repository URL, build the repository on your local web server.
   a) Log in to Broadcom Support.
   b) Download the vCenter Server appliance ISO image. See the Knowledge Base KB 36685.
   c) Confirm that the md5sum is correct by using an MD5 checksum tool.
   d) On your Web server, create a repository directory under the root.

      For example, create the `vc_update_repodirectory`.
   e) Extract the ZIP file into the repository directory.

      The extracted files are in the `manifest` and `package-pool` subdirectories.
2. In the vCenter Server Management Interface, click **Update**.
3. Click **Settings**.
4. Select the Repository settings.

Option	Description
Default repository	Uses the default VMware repository URL that is preset for the build profile of the appliance.
Specified repository	Uses a custom repository. You must enter the repository URL, for example, *`https://web_server_name.your_company.com/`*`vc_update_repo`. The repository URL must use a secure protocol such as HTTPS or FTPS.

5. If the specified repository requires authentication, enter the user name and password.
6. (Optional) If you do not want to perform a security certificate check, deselect the **Check Certificate** check box.
   If you trust the URL for the repository, you can choose to bypass the certificate check for the repository URL.
7. Click **OK**.

Install vCenter Server Patches

Install vCenter Server Patches

You can check for and install patches either from an ISO image or directly from a repository URL.

- Log in to the vCenter Server Management Interface as root.

- Before you can install available patches, you check for new patches and stage the patches to the vCenter Server appliance. See Check for and Stage Patches to the vCenter Server Appliance.
- If you are patching the appliance from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Client. See *vSphere Virtual Machine Administration*.
- If you are patching the appliance from a repository URL, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure the Repository for URL-Based Patching.
- Create an image-based backup and take a powered-off snapshot of the vCenter Server Appliance you are patching as a precaution in case there is a failure during the patching process.

Important: The services running in the vCenter Server appliance become unavailable during the installation of the patches. You must perform this procedure during a maintenance period. As a precaution if there is a failure, you can back up the vCenter Server. For information on backing up and restoring vCenter Server, see *vCenter Server Installation and Setup*.

1. In the vCenter Server Management Interface, click **Update**.

   In the **Current version details** pane, you can view the vCenter Server version and build number.

   In the **Available updates** pane, you can view the available updates with update priority and severity.

   The update priority indicates how soon you must install the update. The values include:

   - **HIGH** - Install as soon as possible.
   - **MEDIUM** - Install at the earliest convenience.
   - **LOW** - Install at your discretion.

   The **Update severity** defines the severity of the issues fixed in the update. The values include the following:

   - **CRITICAL** - Vulnerabilities that can be exploited by an unauthenticated attacker from the Internet or those that break the guest/host Operating System isolation. The exploitation results in the complete compromise of confidentiality, integrity, and availability of user data and/or processing resources without user interaction. Exploitation could be leveraged to propagate an Internet worm or execute arbitrary code between Virtual Machines and/or the Host Operating System.
   - **IMPORTANT** - Vulnerabilities that are not rated critical but whose exploitation results in the complete compromise of confidentiality and/or integrity of user data and/or processing resources through user assistance or by authenticated attackers. This rating also applies to those vulnerabilities which could lead to the complete compromise of availability when exploitation is by a remote unauthenticated attacker from the Internet or through a breach of virtual machine isolation.
   - **MODERATE** - Vulnerabilities where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios could still lead to the compromise of confidentiality, integrity, or availability of user data and/or processing resources.
   - **LOW** - All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.

2. Select the range of staged patches to apply and click **Install**.

   Important: Some updates might require a reboot of the system. You can see information about these updates in the Available Updates pane.

3. Read and accept the End User License Agreement.

4. A system pre-check verifies that the patches can be successfully installed with the provided information.

   If the pre-check discovers missing or incorrect information, or other problems preventing a successful installation, you are prompted to correct the problem and resume the installation.

5. After the installation finishes, click **OK**.
6. If the patch installation requires the appliance to reboot, click **Summary**, and click **Reboot** to reset the appliance.

In the Available Updates pane, you can see the changed update status of the vCenter Server appliance.

Enable Automatic Checks for vCenter Server Patches

You can configure vCenter Server to perform automatic checks for available patches in the configured repository URL at a regular interval.

- Log in to the vCenter Server Management Interface as root.
- Verify that you have configured the repository settings and that the current repository URL is accessible. See Configure the Repository for URL-Based Patching.

1. In the vCenter Server Management Interface, click **Update**.
2. Click **Settings**.
3. Select **Check for updates automatically**, and select the day and time in UTC to perform automatic checks for available patches.
4. Click **OK**.

vCenter Server appliance performs regular checks for available patches in the configured repository URL. In the Available Updates pane, you can view information about the available patches. You can also view the vCenter Server health status for notifications about available patches. See *vCenter Server Configuration*.

Patching the vCenter Server Appliance by Using the Appliance Shell

You can use the `software-packages` utility in the appliance shell of a vCenter Server appliance to see the installed patches, stage new patches, and install new patches.

To perform ISO-based patching, you download an ISO image, mount the ISO image to the CD/DVD drive of the appliance, optionally stage the available patches from the ISO image to the appliance, and install the patches. For steps to mount the ISO image to the CD/DVD drive, see Configure a Datastore ISO File for the CD/DVD Drive section in the vSphere Virtual Machine Administration.

To perform URL-based patching, you optionally stage the available patches from a repository URL to the appliance and install the patches. The vCenter Server appliance is preset with a default VMware repository URL for the build profile of the appliance. You can use the `update.set` command to configure the appliance to use the default VMware repository URL or a custom repository URL, for example, a repository URL that you previously built on a local Web server running within your data center. You can also use the `proxy.set` command to configure a proxy server for the connection between the vCenter Server appliance and the repository URL.

View a List of All Installed Patches in the vCenter Server Appliance

You can use the `software-packages` utility to see a list of the patches currently applied to the vCenter Server appliance. You can also view the list of the installed patches in chronological order and details about a specific patch.

1. Access the appliance shell and log in as a user who has a super administrator role.

   The default user with a super administrator role is root.
2. To view the full list of patches and software packages installed in the vCenter Server appliance, run the following command:

   ```
   software-packages list
   ```

3. To view all patches applied to the vCenter Server appliance in chronological order, run the following command:

   ```
   software-packages list --history
   ```

   You see the list in chronological order. A single patch in this list can be an update of multiple different packages.

4. To view details about a specific patch, run the following command:

   ```
   software-packages list --patch patch_name
   ```

   For example, if you want to view the details about the VMware-vCenter-Server-Appliance-Patch1 patch, run the following command:

   ```
   software-packages list --patch VMware-vCenter-Server-Appliance-Patch1
   ```

   You can see the complete list of details about the patch, such as vendor, description, and installation date.

Configure URL-Based Patching

For URL-based patching, the vCenter Server appliance is preset with a default VMware repository URL for the build profile of the appliance. You can use the `update.set` command to configure the appliance to use the default or a custom repository URL as the current source of patches and enable automatic checks for patches.

By default the current repository for URL-based patching is the default VMware repository URL.

Note: You can use the `proxy.set` command to configure a proxy server for the connection between vCenter Server and the repository URL. For more information about the API commands in the appliance shell, see *vCenter Server Configuration*.

If vCenter Server is not connected to the Internet or if your security policy requires it, you can build and configure a custom repository. The custom patching repository runs on a local Web server within your data center and replicates the data from the default repository. Optionally, you can set up an authentication policy for accessing the Web server that hosts the custom patching repository.

1. If you want to configure a custom repository URL, build the repository on your local Web server.
   a) Download the vCenter Server Appliance patch ZIP file from the VMware website at https://my.vmware.com/web/vmware/downloads.
   b) On your Web server, create a repository directory under the root.
   For example, create the `vc_update_repo` directory.
   c) Extract the ZIP file into the repository directory.
   The extracted files are in the `manifest` and `package-pool` subdirectories.

2. Access the appliance shell and log in as a user who has a super administrator role.
   The default user with a super administrator role is root.

3. To see information about the current URL-based patching settings, run the `update.get` command.
   You can see information about the current repository URL, the default repository URL, the time at which the appliance last checked for patches, the time at which the appliance last installed patches, and the current configuration of automatic checks for patches.

4. Configure the current repository for URL-based patching.
   - To configure the appliance to use the default VMware repository URL, run the following command:

     ```
     update.set --currentURL default
     ```

   - To configure the appliance to use a custom repository URL, run the following command:

     ```
     update.set --currentURL https://web_server_name.your_company.com/vc_update_repo [--username username]
      [--password password]
     ```

     The square brackets [] enclose the command options.

     If the custom repository requires authentication, use the `--username` *username* and `--password` *password* options.

5. To activate automatic checks for vCenter Server appliance patches in the current repository URL at regular intervals, run the following command:

   ```
   update.set --CheckUpdates enabled [--day day] [--time HH:MM:SS]
   ```

   The square brackets [] enclose the command options.

   Use the `--day day` option to set the day for performing the regular checks for patches. You can set a particular day of the week, for example, `Monday` , or `Everyday` . The default value is `Everyday` .

   Use the `--time HH:MM:SS` option to set the time in UTC for performing the regular checks for patches. The default value is `00:00:00` .

   The appliance performs regular checks for available patches in the current repository URL.

6. To deactivate automatic checks for vCenter Server patches, run the following command:

   ```
   update.set --CheckUpdates disabled
   ```

If you configured the appliance to perform automatic checks for available patches, you can regularly view the vCenter Server appliance health status for notifications about available patches. See *vCenter Server Configuration*.

Stage Patches to the vCenter Server Appliance

Before you install available patches, you can stage the patches to the appliance. You can use the `software-packages` utility to stage patches either from a local repository by attaching an ISO image to the appliance, or from a remote repository directly by using a repository URL.

- If you are staging patches from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Client. See *vSphere Virtual Machine Administration*.
- If you are staging patches from a remote repository, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure URL-Based Patching.

1. Access the appliance shell and log in as a user who has a super administrator role.

   The default user with a super administrator role is root.

2. Stage the patches.
   - To stage the patches included in the attached ISO image, run the following command:
     ```
     software-packages stage --iso
     ```
   - To stage the patches included in the current repository URL, run the following command:
     ```
     software-packages stage --url
     ```
     By default the current repository URL is the default VMware repository URL.

     If you want to stage only the third-party patches, use the `--thirdParty` option.
   - To stage the patches included in a repository URL that is not currently configured in the appliance, run the following command:
     ```
     software-packages stage --url URL_of_the_repository
     ```
     If you want to stage only the third-party patches, use the `--thirdParty` option.

   If you want to directly accept the End User License Agreement, use the `--acceptEulas` option.

   For example, to stage only the third-party patches from the current repository URL with directly accepting the End User License Agreement, run the following command:
   ```
   software-packages stage --url --thirdParty --acceptEulas
   ```
   In the process of staging, the command validates that a patch is a VMware patch, that the staging area has enough free space, and that the patches are not altered. Only completely new patches or patches for existing packages that can be upgraded are staged.
3. Optional: To see information about the staged patches, run the following command:
   ```
   software-packages list --staged
   ```
   Each patch includes a metadata file that contains information such as patch version, product name, whether a restart of the system is required, and so on.
4. Optional: To view a list of the staged patches, run the following command:
   ```
   software-packages list --staged --verbose
   ```
5. Optional: To unstage the staged patches, run the following command:
   ```
   software-packages unstage
   ```
   All directories and files generated by the staging process are removed.

Install the staged patches. See Install vCenter Server Patches.

Important: If you staged the patches from an ISO image, keep the ISO image attached to the CD/DVD drive of the appliance. The ISO image must be attached to the CD/DVD drive of the appliance throughout the staging and installation processes.

Install vCenter Server Patches

You can use the `software-packages` utility to install the staged patches. You can also use the `software-packages` utility to install patches directly from an attached ISO image or repository URL without staging the patch payload.

- If you are installing staged patches, verify that you staged the correct patch payload. See Stage Patches to the vCenter Server Appliance.
- If you are installing patches that you previously staged from an ISO image, verify that the ISO image is attached to the CD/DVD drive of the vCenter Server appliance. See Stage Patches to the vCenter Server Appliance.
- If you are installing patches directly from an ISO image that you previously downloaded from https://my.vmware.com/group/vmware/patch, you must attach the ISO image to the CD/DVD drive of the vCenter Server Appliance. You can configure the ISO image as a datastore ISO file for the CD/DVD drive of the appliance by using the vSphere Client. See *vSphere Virtual Machine Administration*.

- If you are installing patches directly from a repository, verify that you have configured the repository settings and that the current repository URL is accessible. See Configure URL-Based Patching.
- Create an image-based backup and take a powered-off snapshot of the vCenter Server Appliance you are patching as a precaution in case there is a failure during the patching process.

Important: The services running in the appliance become unavailable during the installation of the patches. You must perform this procedure during a maintenance period. As a precaution in case of failure, you can back up the vCenter Server appliance. For information about backing up and restoring vCenter Server, see *vCenter Server Installation and Setup*.

1. Access the appliance shell and log in as a user who has a super administrator role.

   The default user with a super administrator role is root.

2. Install the patches.

   - To install staged patches, run the following command:
     ```
     software-packages install --staged
     ```
   - To install patches directly from an attached ISO image, run the following command:
     ```
     software-packages install --iso
     ```
   - To install patches directly from the current repository URL, run the following command:
     ```
     software-packages install --url
     ```

     By default the current repository URL is the default VMware repository URL.
   - To install patches directly from a repository URL that is not currently configured, run the following command:
     ```
     software-packages install --url URL_of_the_repository
     ```

   If you want to directly accept the End User License Agreement, use the `--acceptEulas` option.

   For example, to install patches from the current repository URL without staging the patches with directly accepting the End User License Agreement, run the following command:
   ```
   software-packages install --url --acceptEulas
   ```

3. If the patch installation requires a reboot of the appliance, run the following command to reset the appliance.
   ```
   shutdown now -r "patch reboot"
   ```

Patch a vCenter High Availability Environment

To patch a vCenter Server Appliance configured in a vCenter High Availability (HA) cluster, you must remove the vCenter Server High Availability configuration and delete the Passive and Witness nodes. After patching the vCenter Server Appliance, you must re-create your vCenter Server High Availability clusters.

This procedure describes how to remove the vCenter HA configuration.

1. In the vSphere Client, log in to the vCenter Server from which you want to remove the vCenter HA configuration.
2. Click the **Configure** tab, and select **vCenter HA**.
3. Select **Remove vCenter HA** .
   - The vCenter HA cluster's configuration is removed from the Active, Passive, and Witness nodes.
   - The Active node continues to run as a standalone vCenter Server Appliance.
4. Delete the Passive and Witness nodes.

Patch the vCenter Server Appliance as described in either Patching vCenter Server Using the vCenter Server Management Interface or Patching the vCenter Server Appliance by Using the Appliance Shell.

After patching the vCenter Server Appliance, you can configure vCenter HA. For information about configuring vCenter HA, see *vSphere Availability*.

Troubleshooting a vSphere Upgrade

The installation and upgrade software enables you to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log file. You can also consult the product release notes for known problems.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, review the Update Manager log file `vmware-vum-server-log4cpp.log`.

The *vSphere Ugrade* guide describes how to use VMware products and their features. If you encounter problems or error situations that are not described in this guide, you may find a solution in VMware Knowledge Base. You can also use VMware Community Forums to find others with same problem or ask for help, or you can open Support Request to get help from VMware service professional.

Collect Installation Logs for vCenter Server Appliance

You can collect installation log files and check these files to identify the source of a failure if vCenter Server appliance stops responding during initial startup.

1. Access the vCenter Server appliance shell.

Option	Description
If you have direct access to the appliance	Press Alt+F1.
To connect remotely	Use SSH or another remote console connection to start a session to the appliance.

2. Enter a user name and password that the appliance recognizes.
3. In the appliance shell, run the `pi shell` command to access the Bash shell.
4. In the Bash shell, run the `vc-support.sh` script to generate a support bundle.
   This command generates a `.tgz` file in `/storage/log`.
5. Export the generated support bundle to the `user@x.x.x.x:/tmp` folder.

   ```
   scp /var/tmp/vc-etco-vm-vlan11-dhcp-63-151.eng.vmware.com-2014-02-28--21.11.tgz user@x.x.x.x:/tmp
   ```

6. Determine which `firstboot` script failed.

   ```
   cat /var/log/firstboot/firstbootStatus.json
   ```

To identify potential causes of the failure, examine the log file of the `firstboot` script that failed.

Errors and Warnings Returned by the Installation and Upgrade Precheck Script

The installation and upgrade precheck script runs tests to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final screen of the GUI installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors and warnings are written to the installation log file.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, review the Update Manager log file `vmware-vum-server-log4cpp.log`.

Table 93: Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script

Error or Warning	Description
64BIT_LONGMODESTATUS	The host processor must be 64-bit.
COS_NETWORKING	Warning. An IPv4 address was found on an enabled service console virtual NIC that has no corresponding address in the same subnet in the VMkernel. A separate warning appears for each such occurrence.
CPU_CORES	The host must have at least two cores.
DISTRIBUTED_VIRTUAL_SWITCH	If the Cisco Virtual Ethernet Module (VEM) software is found on the host, the test checks that the upgrade also contains the VEM software. The test also determines whether the upgrade supports the same version of the Cisco Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the test returns a warning. The result indicates which version of the VEM software was expected on the upgrade ISO and which versions, if any, were found. You can use ESXi Image Builder CLI to create a custom installation ISO that includes the appropriate version of the VEM software.
HARDWARE_VIRTUALIZATION	Warning. If the host processor does not have hardware virtualization, or if hardware virtualization is not turned on in the host BIOS, host performance suffers. You can enable hardware virtualization in the host machine boot options panel. See your hardware vendor's documentation.
MD5_ROOT_PASSWORD	This test checks that the root password is encoded in MD5 format. If a password is not encoded in MD5 format, it might be significant only to eight characters. In this case, any characters after the first eight are no longer authenticated after the upgrade, which can create a security problem. To work around this problem, see Knowledge Base article KB 1024500.
MEMORY_SIZE	The host requires the specified amount of memory to upgrade.
PACKAGE_COMPLIANCE	vSphere Update Manager upgrade to vSphere Lifecycle Manager only. This test checks the existing software on the host against the software contained on the upgrade ISO to determine whether the host has been successfully upgraded. If any of the packages are missing or are an older version than the package on the upgrade ISO, the test returns an error. The test results indicate which software was found on the host and which software was found on the upgrade ISO.
PARTITION_LAYOUT	You can upgrade or migrate software only if at most one VMFS partition on the disk is being upgraded. The VMFS partition must begin after sector 1843200.

Error or Warning	Description
POWERPATH	This test checks for the installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the test checks that matching components, such as CIM or the VMkernel and module, also exist in the upgrade. If they do not exist, the test returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found.
PRECHECK_INITIALIZE	This test checks that the precheck script can be run.
SANE_ESX_CONF	The `/etc/vmware/esx.conf` file must exist on the host.
SPACE_AVAIL_ISO	vSphere Update Manager only. The host disk must have enough free space to store the contents of the installer CD or DVD.
SPACE_AVAIL_CONFIG	vSphere Update Manager upgrade to vSphere Lifecycle Manager only. The host disk must have enough free space to store the legacy configuration between reboots.
SUPPORTED_ESX_VERSION	You can upgrade or migrate to ESXi7.0 only from version 6.0 ESXi hosts.
TBOOT_REQUIRED	This message applies only to vSphere Update Manager upgrade to vSphere Lifecycle Manager only. The upgrade fails with this error when the host system is running in trusted boot mode (tboot), but the ESXi upgrade ISO does not contain any tboot VIBs. This test prevents an upgrade that can make the host less secure.
UNSUPPORTED_DEVICES	Warning. This test checks for unsupported devices. Some PCI devices are not supported in ESXi7.0.
UPDATE_PENDING	This test checks the host for VIB installations that require a reboot. This test fails if one or more such VIBs are installed, but the host has not yet been rebooted. In these conditions, the precheck script is unable to determine reliably which packages are currently installed on the host. If this test fails, it may not be safe to rely on the rest of the precheck tests to determine whether an upgrade is safe. If you encounter this error, restart the host and retry the upgrade.

Upgrade Issues with vCenter Server Containing Host Profiles

Most common issues that might occur during a vCenter Server upgrade to version 7.0, that contains host profiles.

- For issues occurring during a vCenter Server upgrade or ESXi upgrade, see *Troubleshooting a vSphere Upgrade*.
- If upgrading vCenter Server 6.5 or 6.7, containing host profiles with version earlier than 6.5, results with a failure, see KB 52932.
- For error `There is no suitable host in the inventory as reference host for the profile Host Profile. The profile does not have any associated reference host`, see KB 2150534.
- If an error occurs when you import a host profile to an empty vCenter Server inventory, see *vSphere Host Profiles* for Reference Host is Unavailable.
- If a host profile compliance check fails for NFS datastore, see *vSphere Host Profiles* for Host Profile without NFS Datastore.
- If compliance check fails with an error for the UserVars.ESXiVPsDisabledProtocols option, when an ESXi host upgraded to version 7.0 is attached to a host profile with version 6.5, see VMware vSphere 7.0 Release Notes.

Roll Back a vCenter Server Instance on Windows When vCenter Server Upgrade Fails

You can roll back or restore a vCenter Server instance on Windows when an upgrade of vCenter Server with an external Platform Services Controller fails after the export stage and the legacy environment has been uninstalled.

The roll back or restore of vCenter Server applies when all of the following conditions apply:

- You must have access to the vCenter Server for Windows machine.
- The vCenter Server instance is attached to an external Platform Services Controller.
- The upgrade of the vCenter Server instance attached to the Platform Services Controller instance is in a failed state after the export stage and uninstallation of the legacy vCenter Server.
- Ensure that vCenter Server rollback happened properly in case of upgrade failure and that no stale failed upgrade log entries remain.

For Rollback Method 1:

- To clean up vCenter Server appliance 7.0 data from the legacy Platform Services Controller, see KB 2106736.
- Use a vCenter Server database snapshot taken before the start of the vCenter Server upgrade.

For Rollback Method 2:

- Use a powered off snapshot of the vCenter Server before the vCenter Server upgrade.
- Use a Platform Services Controller snapshot taken after the Platform Services Controller node upgrade and before the start of the vCenter Server upgrade.
- Use a vCenter Server snapshot taken after the Platform Services Controller upgrade and before the start of the vCenter Server upgrade.

You can restore the legacy vCenter Server using Rollback Method 1 or Rollback Method 2.

- Use Rollback Method 1.
  a. Manually clean up vCenter Server appliance data from Platform Services Controller.
  b. Restore the legacy vCenter Server database from a backup which was taken before the upgrade.
  c. Point the legacy vCenter Server instance to the Platform Services Controller, and also point to the database with the restored data.
  d. Ensure that the vCenter Server services are up and running.
- Use Rollback Method 2.
  a. Restore the Platform Services Controller instance from a snapshot to the point where you were about to start vCenter Server upgrade. You can use a backup for a Windows configuration or use another backup and restore approach to revert the snapshot.
  b. Restore the vCenter Server instance from a snapshot.
  c. Restore the vCenter Server database from a snapshot.
  d. Ensure that the vCenter Server services are up and running.

For Rollback Method 2, you will lose all data written to Platform Services Controller after the vCenter Server upgrade has been started when you restore from the Platform Services Controller snapshot taken before that point in time.

Collect Logs to Troubleshoot ESXi Hosts

You can collect installation or upgrade log files for ESXi. If an installation or upgrade fails, checking the log files can help you identify the source of the failure.

1. Enter the `vm-support` command in the ESXi Shell or through SSH.
2. Navigate to the `/var/tmp/` directory.
3. Retrieve the log files from the `.tgz` file.

vSphere Authentication

The *vSphere Authentication* documentation provides information to help you perform common tasks such as certificate management and vCenter Single Sign-On configuration.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

vSphere Authentication explains how you can manage certificates for vCenter Server and related services, and set up authentication with vCenter Single Sign-On.

Table 94: *vSphere Authentication* Highlights

Topics	Content Highlights
Getting Started with Authentication	• Managing authentication services. • Managing vCenter Server using the vCenter Server Management Interface.
vSphere Security Certificates	• Certificate model, and options for replacing certificates. • Replace certificates from the UI (simple cases). • Replace certificates using the Certificate Manager utility. • Replace certificates using the CLI (complex situations). • Certificate management CLI reference.
vSphere Authentication with vCenter Single Sign-On	• Architecture of the authentication process. • How to add identity sources so users in your domain can authenticate. • Two-factor authentication. • Managing users, groups, and policies. • vCenter Server Identity Provider Federation

What Happened to the Platform Services Controller

Beginning in vSphere 7.0, deploying a new vCenter Server or upgrading to vCenter Server 7.0 requires the use of the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server appliance, see the *vSphere Upgrade* documentation.

Related Documentation

A companion document, *vSphere Security*, describes available security features and the measures that you can take to safeguard your environment from attack. That document also explains how you can set up permissions, and includes a reference to privileges.

In addition to these documents, VMware publishes the *vSphere Security Configuration Guide* (formerly known as the *Hardening Guide*) for each release of vSphere, accessible at https://core.vmware.com/security. The *vSphere Security Configuration Guide* contains guidelines on security settings that can or should be set by the customer, and security settings delivered by VMware that should be audited by the customer to ensure that they are still set to default.

Intended Audience

This information is intended for administrators who want to configure vCenter Server authentication and manage certificates. The information is written for experienced Linux system administrators who are familiar with virtual machine technology and data center operations.

Updated Information

This *vSphere Authentication* document is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Authentication* documentation.

Revision	Description
08 MAY 2024	• Minor update to Active Directory over LDAP and OpenLDAP Server Identity Source Settings. • Minor update to dir-cli Command Reference.
30 JAN 2024	• Minor update to Solution User Certificates. • Minor update to VMware Endpoint Certificate Store Overview.
19 JAN 2024	• Minor update to Configure vCenter Server Smart Card Authentication to Request Client Certificates.
12 JAN 2024	• Minor update to Replace Solution User Certificates with New VMCA-Signed Certificates. • Updated the steps in Replace Machine SSL Certificates with Custom Certificates. • Updated the Active Directory over LDAP and OpenLDAP Server Settings table with additional information about LDAPS certificates in Active Directory over LDAP and OpenLDAP Server Identity Source Settings.
21 DEC 2023	• Minor update to Add a Trusted Root Certificate to the Certificate Store.
22 NOV 2023	• Updated Replace Solution User Certificates with New VMCA-Signed Certificates and certool Management Commands Reference to indicate that the `--config <config_file>` option is required. • Minor update to Add or Edit a vCenter Single Sign-On Identity Source. • Updated Configure vCenter Server Smart Card Authentication to Request Client Certificates with information about port 3128.
01 MAY 2023	• Minor update to Edit the vCenter Single Sign-On Password Policy. • Minor update to Use the vSphere Client to Manage Smart Card Authentication.
27 FEB 2023	• Updated information about AD FS certificates in Configure vCenter Server Identity Provider Federation for AD FS.

Revision	Description
	• Updated the descriptions for the SystemConfiguration.BashShellAdministrators, SystemConfiguration.Administrators, and SystemConfiguration.ReadOnly groups in Groups in the vCenter Single Sign-On Domain.
10 FEB 2023	• Minor update to Certificate Requirements for Different Solution Paths.
09 FEB 2023	• Updated Groups in the vCenter Single Sign-On Domain to include missing group information. • Minor updates to smart card information in Configuring and Using Smart Card Authentication and Configure vCenter Server Smart Card Authentication to Request Client Certificates.
10 JAN 2023	• Minor update to Configure vCenter Server Smart Card Authentication to Request Client Certificates.
05 JAN 2023	• Minor update to Configure vCenter Server Smart Card Authentication to Request Client Certificates.
22 DEC 2022	• Minor update to Active Directory over LDAP and OpenLDAP Server Identity Source Settings. • Minor update to Configure vCenter Server Smart Card Authentication to Request Client Certificates.
30 NOV 2022	• Minor update to Manage vCenter Server with the Management Interface. • Minor update to dir-cli Command Reference.
01 NOV 2022	• Minor update to Active Directory over LDAP and OpenLDAP Server Identity Source Settings.
11 OCT 2022	• Minor update to Replace Solution User Certificates with New VMCA-Signed Certificates.
27 JUL 2022	• Minor update to Certificate Requirements for Different Solution Paths. • Added information about SMS self-signed certificates to Where vSphere Uses Certificates.
06 MAY 2022	• Minor update to Certificate Management Overview. • Minor update to Regenerate a New VMCA Root Certificate and Replace All Certificates.
21 JAN 2022	• Updated vCenter Server Identity Provider Federation Caveats and Interoperability and Configure vCenter Server Identity Provider Federation for AD FS with additional information.
17 DEC 2021	• Minor update to Certificate Requirements for Different Solution Paths. • Minor update to Make VMCA an Intermediate Certificate Authority (Certificate Manager).
05 OCT 2021	Initial release.

Getting Started with Certificate Management and Authentication

vCenter Server provides common infrastructure services to the vSphere environment, including certificate management and authentication with vCenter Single Sign-On.

vSphere Certificate Management and Authentication Overview

vSphere provides services that enable you to perform certificate management tasks for vCenter Server and ESXi components, and configure authentication through vCenter Single Sign-On.

vSphere Certificate Management Overview

By default, vSphere enables you to provision vCenter Server components and ESXi hosts with VMware Certificate Authority (VMCA) certificates. You can also use custom certificates, which are stored in the VMware Endpoint Certificate Store (VECS).

vCenter Single Sign-On Overview

vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism. vCenter Single Sign-On uses specific terms and definitions that are important to understand.

Table 95: vCenter Single Sign-On Glossary

Term	Definition
Principal	An entity that can be authenticated, such as a user.
Identity Provider	A service that manages identity sources and authenticates principals. Examples: Microsoft Active Directory Federation Services (AD FS) and vCenter Single Sign-On.
Identity Source (Directory Service)	Stores and manages principals. Principals consist of a collection of attributes about a user or service account such as name, address, email, and group membership. Examples: Microsoft Active Directory and VMware Directory Service (vmdir).
Authentication	The means of determining whether someone or something is, in fact, who or what it declares itself to be. For example, users are authenticated when they provide their credentials, such as smart cards, user name and correct password, and so on.
Authorization	The process of verifying what objects principals have access to.
Token	A signed collection of data comprising the identity information for a given principal. A token might include not only basic information about the principal such as email address and full name, but also, depending on the token type, the principal's groups and roles.
vmdir	VMware Directory Service. The internal (local) LDAP repository in vCenter Server that contains user identities, groups, and configuration data.
OpenID Connect (OIDC)	Authentication protocol based on OAuth2. vCenter Server uses OIDC capabilities when interacting with Active Directory Federation Services (AD FS).

vCenter Single Sign-On Authentication Types

vCenter Single Sign-On uses different types of authentication, depending on whether the built-in vCenter Server identity provider or an external identity provider is involved.

Table 96: vCenter Single Sign-On Authentication Types

Authentication Type	What Acts as the Identity Provider?	Does vCenter Server Handle the Password?	Description
Token-Based Authentication	External identity provider. For example, AD FS.	No	vCenter Server contacts the external identity provider through a particular protocol and obtains a token, which represents a particular user identity.
Simple Authentication	vCenter Server	Yes	The user name and password are passed directly to vCenter Server, which validates the credentials through its identity sources.

Managing Certificates

You manage certificates from the vSphere Client, or by using an API, scripts, or CLIs.

You can manage certificates using different interfaces.

Table 97: Interfaces for Managing Certificates

Interface	Description
vSphere Client	Web interface (HTML5-based client). See Managing Certificates with the vSphere Client.
vSphere Automation API	See *VMware vSphere Automation SDKs Programming Guide*.
Certificate Management utility	Command-line tool that supports Certificate Signing Request (CSR) generation and certificate replacement. See Managing Certificates with the vSphere Certificate Manager Utility.
CLIs for managing certificate and directory services	Set of commands for managing certificates, the VMware Endpoint Certificate Store (VECS), and VMware Directory Service (vmdir). See Managing Services and Certificates with CLI Commands.

Manage Certificates from the vSphere Client

You can manage certificates from the vSphere Client.

1. Log in to a vCenter Server as a user with administrator privileges in the local vCenter Single Sign-On domain. The default domain is vsphere.local.
2. Select **Administration**.
3. Under **Certificates**, click **Certificate Management**.
   Certificate panels for the different types of certificates appear.

4. Perform certificate tasks, such as viewing certificate details, renewing the Machine SSL certificate, and adding a Trusted Root certificate.

Use Scripts to Manage Certificates

vCenter Server includes scripts for generating Certificate Signing Requests (CSRs), managing certificates, and managing services.

Enable SSH login to vCenter Server. See Manage vCenter Server with the Management Interface.

For example, you can use the `certool` utility to generate CSRs and to replace certificates. See Managing Certificates with the vSphere Certificate Manager Utility.

Use the CLIs for management tasks that the vSphere Client does not support, or to create custom scripts for your environment.

Table 98: CLIs for Managing Certificates and Associated Services

CLI	Description	Links
`certool`	Generate and manage certificates and keys. Part of VMware Certificate Authority (VMCA).	certool Initialization Commands Reference
`vecs-cli`	Manage the contents of VMware Certificate Store instances. Part of VMware Authentication Framework Daemon (VMAFD).	vecs-cli Command Reference
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	dir-cli Command Reference
`sso-config`	Update Security Token Service (STS) certificates.	Replace a vCenter Server STS Certificate Using the Command Line
`service-control`	Command for starting, stopping, and listing services.	Run this command to stop services before running other CLI commands.

1. Log in to the vCenter Server shell.

   Usually, you have to be the root or Administrator user. See Required Privileges for Running CLIs for details.

2. Access a CLI at one of the following default locations.

   The required privileges depend on the task that you want to perform. Sometimes, you are prompted for the password twice to safeguard sensitive information.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli
   /usr/lib/vmware-vmafd/bin/dir-cli
   /usr/lib/vmware-vmca/bin/certool
   /opt/vmware/bin
   /opt/vmware/bin/sso-config.sh
   ```

   The `service-control` command does not require that you enter the path.

Managing Authentication Services

You manage authentication services from the vSphere Client, or by using the CLI. You can also manage the vCenter Server Identity Provider Federation configuration process by using an API.

You can manage authentication using different interfaces.

Table 99: Interfaces for Managing Authentication Services

Interface	Description
vSphere Client	Web interface (HTML5-based client).
API	Manage the vCenter Server Identity Provider Federation configuration process.
`sso-config`	Command-line utility for configuring the vCenter Server built-in identity provider.

Manage Authentication Services from the vSphere Client

You can manage vCenter Server authentication services from the vSphere Client.

1. Log in to a vCenter Server as a user with administrator privileges in the local vCenter Single Sign-On domain.
   The default domain is vsphere.local.
2. Select **Administration**.
3. Under **Single Sign On**, click **Configuration** to manage identity providers and configure password and lockout policies.

Use Scripts to Manage Authentication Services

vCenter Server includes a utility, `sso-config`, for managing authentication services.

Enable SSH login to vCenter Server. See Manage vCenter Server with the Management Interface.

Use the `sso-config` utility for management tasks that the vSphere Client does not support, or to create custom scripts for your environment.

Table 100: CLIs for Managing Authentication and Associated Services

CLI	Description	Links
`sso-config`	Command-line utility for configuring the vCenter Server built-in identity provider.	Refer to the `sso-config` help by running `sso-config.sh -help`, or see the VMware knowledge base article at https://kb.vmware.com/s/article/67304 for usage examples.
`service-control`	Command for starting, stopping, and listing services.	Run this command to stop services before running other CLI commands.

1. Log in to the vCenter Server shell.
   Usually, you have to be the root or Administrator user. See Required Privileges for Running CLIs for details.
2. Access the `sso-config` utility at following default location.
   The required privileges depend on the task that you want to perform. Sometimes, you are prompted for the password twice to safeguard sensitive information.
   ```
   /opt/vmware/bin/sso-config.sh
   ```
   The `service-control` command does not require that you specify the path.

Managing the vCenter Server

You can manage the vCenter Server from the vCenter Server Management Interface or from the vCenter Server shell.

For more information about managing vCenter Server, see *vCenter Server Configuration*.

Table 101: Interfaces for Managing the vCenter Server

Interface	Description
vCenter Server Management Interface	Use this interface to reconfigure the system settings. See Manage vCenter Server with the Management Interface.
vCenter Server shell	Use this command-line interface to perform service management operations on VMCA, VECS, and VMDIR. See Managing Certificates with the vSphere Certificate Manager Utility and Managing Services and Certificates with CLI Commands.

Manage vCenter Server with the Management Interface

You can use the vCenter Server Management Interface to configure the system settings.

Settings include time synchronization, network settings, and SSH login settings. You can also change the root password, join the appliance to an Active Directory domain, and leave an Active Directory domain.
Note: Under the **Networking** pane, the virtual NIC 0 is reserved for management traffic. You cannot reassign the traffic from NIC 0 to another NIC. If you are using VCHA, this traffic uses NIC 1. You can add NICs to the vCenter Server Appliance. See the VMware knowledge base article at https://kb.vmware.com/article/2147155.

1. In a browser, go to the Web interface at `https://vcenter_server_ip:5480`.
2. If a warning message about an untrusted SSL certificate appears, resolve the issue based on your company security policy and the browser that you are using.
3. Log in as root.
   The default root password is the root password that you set when deploying the vCenter Server.

You see the Summary page of the vCenter Server Management Interface.

Manage vCenter Server from the vCenter Server Shell

You can use service management utilities and CLIs from the vCenter Server shell. You can use TTY1 to log in to the console, or can use SSH to connect to the shell.

1. Enable SSH login if necessary.
   a) Log in to the vCenter Server Management Interface at https://*vcenter_server_ip*:5480.
   b) In the Navigator, select **Access** and click **Edit**.
   c) Toggle on **Enable SSH Login** and click **OK**.
   You can follow the same steps to enable the Bash shell for the vCenter Server.
2. Access the shell.
   - If you have direct access to the vCenter Server console, select **Log in**, and press Enter.
   - To connect remotely, use SSH or another remote console connection to start a session to the vCenter Server.
3. Log in as root with the password that you set when you initially deployed the vCenter Server.
   If you changed the root password, use the new password.

Add a vCenter Server to an Active Directory Domain

If you want to add an Active Directory identity source to vCenter Server, you must join the vCenter Server to an Active Directory domain.

If you are unable to use vCenter Server Identity Provider Federation, or Active Directory over LDAPS, vCenter Server supports Integrated Windows Authentication (IWA). To use IWA, you must join the vCenter Server to your Active Directory domain.

1. Using the vSphere Client, log in to vCenter Server as a user with administrator privileges in the local vCenter Single Sign-On domain (vsphere.local by default).
2. Select **Administration**.
3. Expand **Single Sign On** and click **Configuration**.
4. Under the **Identity Provider** tab, click **Active Directory Domain**.
5. Click **Join AD**, enter the domain, optional organizational unit, and user name and password, and click **Join**.
6. Restart vCenter Server.

To attach users and groups from the joined Active Directory domain, add the joined domain as a vCenter Single Sign-On identity source. See Add or Edit a vCenter Single Sign-On Identity Source.

vSphere Security Certificates

vSphere provides security by using certificates to encrypt communications, authenticate services, and sign tokens.

vSphere uses certificates to:

- Encrypt communications between two nodes, such as a vCenter Server and an ESXi host.
- Authenticate vSphere services.
- Perform internal actions such as signing tokens.

vSphere's internal certificate authority, VMware Certificate Authority (VMCA), provides all the certificates necessary for vCenter Server and ESXi. VMCA is installed on every vCenter Server host, immediately securing the solution without any other modification. Keeping this default configuration provides the lowest operational overhead for certificate management. vSphere provides a mechanism to renew these certificates in the event they expire.

vSphere also provides a mechanism to replace certain certificates with your own certificates. However, replace only the SSL certificate that provides encryption between nodes, to keep your certificate management overhead low.

The following options are recommended for managing certificates.

Table 102: Recommended Options for Managing Certificates

Mode	Description	Advantages
VMCA Default Certificates	VMCA provides all the certificates for vCenter Server and ESXi hosts.	Simplest and lowest overhead. VMCA can manage the certificate life cycle for vCenter Server and ESXi hosts.
VMCA Default Certificates with External SSL Certificates (Hybrid Mode)	You replace the vCenter Server SSL certificates, and allow VMCA to manage certificates for solution users and ESXi hosts. Optionally, for high-security conscious deployments, you can replace the ESXi host SSL certificates as well.	Simple and secure. VMCA manages internal certificates but you get the benefit of using your corporate-approved SSL certificates, and having those certificates trusted by your browsers.

VMware does not recommend replacing either solution user certificates or STS certificates, nor using a subordinate CA in place of the VMCA. If you choose either of these options, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

You can use the following options to replace the existing certificates.

Table 103: Different Approaches to Certificate Replacement

Option	See
Use the vSphere Client.	Managing Certificates with the vSphere Client
Use the vSphere Automation API to manage the life cycle of certificates.	*VMware vSphere Automation SDKs Programming Guide*
Use the vSphere Certificate Manager utility from the command line.	Managing Certificates with the vSphere Certificate Manager Utility
Use CLI commands for manual certificate replacement.	Managing Services and Certificates with CLI Commands

Certificate Requirements for Different Solution Paths

Certificate requirements depend on whether you use VMCA as an intermediate CA or you use custom certificates. Requirements are also different for machine certificates.

Before you begin, ensure that all nodes in your environment are time synchronized.

Note: vSphere deploys only RSA certificates for server authentication and does not support generating ECDSA certificates. vSphere verifies ECDSA certificates presented by other servers. For example, if vSphere connects to a syslog server and the syslog server has an ECDSA certificate, vSphere supports verifying that certificate.

Requirements for all Imported Certificates

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When you add keys to VECS, they are converted to PKCS8.
- x509 version 3
- SubjectAltName must contain DNS Name=*machine_FQDN*
- CRT format
- Exempting the vpxd-extension solution user certificate, Extended Key Usage can be either empty or contain Server Authentication.

vSphere does not support the following certificates.

- Certificates with wildcards.
- The algorithms md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1, and sha1WithRSAEncryption are not supported.
- When creating a custom machine SSL certificate for vCenter Server, Server Authentication and Client Authentication are not supported, and must be removed when using the Microsoft Certificate Authority (CA) templates. For more information, see the VMware knowledge base article at https://kb.vmware.com/s/article/2112009.

Certificate Compliance to RFC 2253

The certificate must be in compliance with RFC 2253.

If you do not generate CSRs using Certificate Manager, ensure that the CSR includes the following fields.

String	X.500 AttributeType
CN	`commonName`
L	`localityName`
ST	`stateOrProvinceName`
O	`organizationName`
OU	`organizationalUnitName`
C	`countryName`
STREET	`streetAddress`
DC	`domainComponent`
UID	`userid`

If you generate CSRs using Certificate Manager, you are prompted for the following information, and Certificate Manager adds the corresponding fields to the CSR file.

- The password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.
- Information that Certificate Manager stores in the `certool.cfg` file. For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.
  - Password for administrator@vsphere.local
  - Two-letter country code
  - Company name
  - Organization name
  - Organization unit
  - State
  - Locality
  - IP address (optional)
  - Email
  - Host name, that is, the fully qualified domain name of the machine for which you want to replace the certificate. If the host name does not match the FQDN, certificate replacement does not complete correctly and your environment might end up in an unstable state.
  - IP address of the vCenter Server node on which you run Certificate Manager.

  Note: As of vSphere 7.0 Update 3o, the OU (organizationalUnitName) field is no longer mandatory.

Requirements When Using VMCA as an Intermediate CA

When you use VMCA as an intermediate CA, the certificates must meet the following requirements.

Certificate Type	Certificate Requirements
Root certificate	• You can use vSphere Certificate Manager to create the CSR. See Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA).

Certificate Type	Certificate Requirements

	• If you prefer to create the CSR manually, the certificate that you send to be signed must meet the following requirements.
	  • Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
	  • PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
	  • x509 version 3
	  • The CA extension must be set to true for root certificates, and cert sign must be in the list of requirements. For example:
	  `basicConstraints = critical,CA:true`
	  `keyUsage = critical,digitalSignature,keyCertSign`
	  • CRL signing must be enabled.
	  • Extended Key Usage can be either empty or contain Server Authentication.
	  • No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is 10 certificates.
	  • Certificates with wildcards or with more than one DNS name are not supported.
	  • You cannot create subsidiary CAs of VMCA.
	  See the VMware knowledge base article at http://kb.vmware.com/kb/2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x, for an example using Microsoft Certificate Authority.

Machine SSL certificate	You can use the vSphere Certificate Manager to create the CSR or create the CSR manually. If you create the CSR manually, it must meet the requirements listed previously under *Requirements for All Imported Certificates*. You also have to specify the FQDN for the host.
Solution user certificate	You can use vSphere Certificate Manager to create the CSR or create the CSR manually. **Note:** You must use a different value for Name for each solution user. If you generate the certificate manually, this might show up as **CN** under **Subject**, depending on the tool you use. If you use vSphere Certificate Manager, the tool prompts you for certificate information for each solution user. vSphere Certificate Manager stores the information in `certool.cfg`. See *Information that Certificate Manager Prompts For*. For the vpxd-extension solution user, you can either leave Extended Key Usage empty or use "TLS WWW client authentication".

Requirements for Custom Certificates

When you want to use custom certificates, the certificates must meet the following requirements.

Certificate Type	Certificate Requirements
Machine SSL certificate	The machine SSL certificate on each node must have a separate certificate from your third-party or enterprise CA.

Certificate Type	Certificate Requirements
	• You can generate the CSR using the vSphere Client or vSphere Certificate Manager, or create the CSR manually. The CSR must meet the requirements listed previously under *Requirements for All Imported Certificates*. • For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.
Solution user certificate	Each solution user on each node must have a separate certificate from your third-party or enterprise CA. • You can generate the CSRs using vSphere Certificate Manager or prepare the CSR yourself. The CSR must meet the requirements listed previously under *Requirements for All Imported Certificates*. • If you use vSphere Certificate Manager, the tool prompts you for certificate information for each solution user. vSphere Certificate Manager stores the information in `certool.cfg`. See *Information that Certificate Manager Prompts For*. **Note:** You must use a different value for Name for each solution user. A manually generated certificate might show up as **CN** under **Subject**, depending on the tool you use. When later you replace solution user certificates with custom certificates, provide the complete signing certificate chain of the third-party CA. For the vpxd-extension solution user, you can either leave Extended Key Usage empty or use "TLS WWW client authentication".

Certificate Management Overview

The work required for setting up or updating your certificate infrastructure depends on the requirements in your environment. You must consider whether you are performing a fresh install or an upgrade, and whether you are considering ESXi or vCenter Server.

Administrators Who Do Not Replace VMware Certificates

VMCA can handle all certificate management. VMCA provisions vCenter Server components and ESXi hosts with certificates that use VMCA as the root certificate authority. If you are upgrading to vSphere 6 from an earlier version of vSphere, all self-signed certificates are replaced with certificates that are signed by VMCA.

If you do not currently replace VMware certificates, your environment starts using VMCA-signed certificates instead of self-signed certificates.

Administrators Who Replace VMware Certificates with Custom Certificates

If your company policy requires certificates that are signed by a third-party or enterprise CA, or that require custom certificate information, you have several choices for a fresh installation.

- Have the VMCA root certificate signed by a third-party CA or enterprise CA. Replace the VMCA root certificate with that signed certificate. In this scenario, the VMCA certificate is an intermediate certificate. VMCA provisions vCenter Server components and ESXi hosts with certificates that include the full certificate chain.
- If your company policy does not allow intermediate certificates in the chain, you can replace certificates explicitly. You can use the vSphere Client, vSphere Certificate Manager utility, or perform manual certificate replacement using the certificate management CLIs.

When upgrading an environment that uses custom certificates, you can retain some of the certificates.

- ESXi hosts keep their custom certificates during upgrade. Make sure that the vCenter Server upgrade process adds all the relevant root certificates to the TRUSTED_ROOTS store in VECS on the vCenter Server.
  After the upgrade to vSphere 6.0 or later, you can set the certificate mode to **Custom**. If the certificate mode is VMCA, the default, and the user performs a certificate refresh from the vSphere Client, the VMCA-signed certificates replace the custom certificates.
- For an upgrade of a simple vCenter Server installation to an embedded deployment, vCenter Server retains custom certificates. After the upgrade, your environment works as before. The existing vCenter Server and vCenter Single Sign-On certificates are retained. The certificates are used as machine SSL certificates. In addition, VMCA assigns a VMCA-signed certificate to each solution user (collection of vCenter services). The solution user uses this certificate only to authenticate to vCenter Single Sign-On. Replacing solution user certificates is often not required by a company policy.
  You can use the command-line utility, vSphere Certificate Manager, for most certificate management tasks.

vSphere Certificate Interfaces

For vCenter Server, you can view and replace certificates with the following tools and interfaces.

Table 104: Interfaces for Managing vCenter Server Certificates

Interface	Use
vSphere Client	Perform common certificate tasks with a graphical user interface.
vSphere Automation API	See *VMware vSphere Automation SDKs Programming Guide*.
Certificate Manager utility	Perform common certificate replacement tasks from the command line of the vCenter Server installation.
Certificate management CLIs	Perform all certificate management tasks with `dir-cli`, `certool`, and `vecs-cli`.
`sso-config` utility	Perform STS certificate management from the command line of the vCenter Server installation.
PowerCLI 12.4 (requires vSphere 7.0 or later)	Perform trusted certificate store management, manage vCenter Server Machine SSL certificates, and manage ESXi Machine SSL certificates.

For ESXi, you perform certificate management from the vSphere Client. VMCA provisions certificates and stores them locally on the ESXi host. VMCA does not store ESXi host certificates in VMDIR or in VECS. See the *vSphere Security* documentation.

Supported vCenter Certificates

For vCenter Server and related machines and services, the following certificates are supported:

- Certificates that are generated and signed by VMware Certificate Authority (VMCA).
- Custom certificates.
  - Enterprise certificates that are generated from your own internal PKI.
  - Third-party CA-signed certificates that are generated by an external PKI such as Verisign, GoDaddy, and so on.

Self-signed certificates that were created using OpenSSL in which no Root CA exists are not supported.

Certificate Replacement Overview

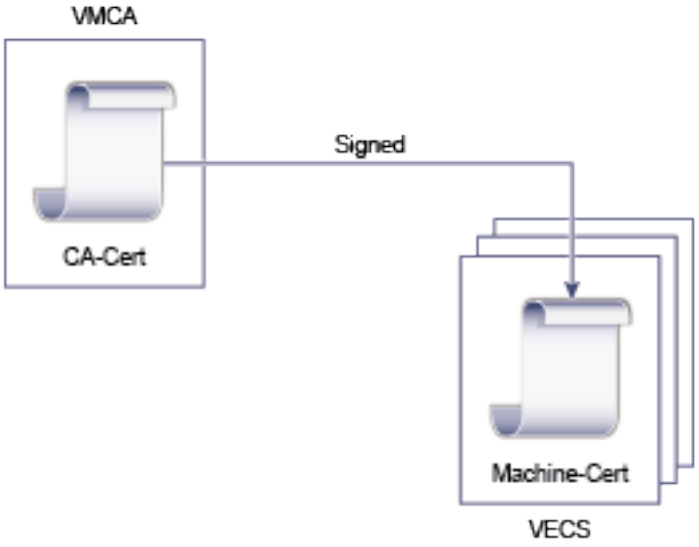
You can perform different types of certificate replacement depending on your company policy and requirements for the system that you are configuring. You can perform certificate replacement from the vCenter Server, by using the vSphere Certificate Manager utility, or manually by using the CLIs included with your installation.

You can replace the default certificates. For vCenter Server components, you can use a set of command-line tools included in your installation. You have several options.

Replace with Certificates Signed by VMCA

If your VMCA certificate expires or you want to replace it for other reasons, you can use the certificate management CLIs to perform that process. By default, the VMCA root certificate expires after 10 years, and all certificates that VMCA signs expire when the root certificate expires, that is, after a maximum of 10 years.

Figure 41: Certificates Signed by VMCA Are Stored in VECS

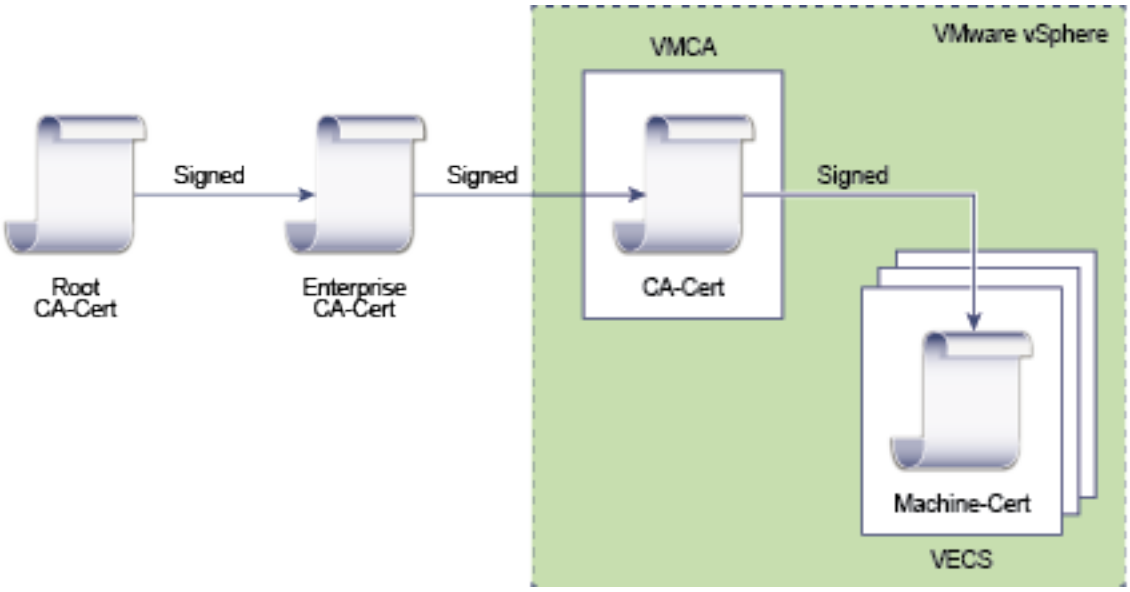


Make VMCA an Intermediate CA

You can replace the VMCA root certificate with a certificate that is signed by an enterprise CA or third-party CA. VMCA signs the custom root certificate each time it provisions certificates, making VMCA an intermediate CA.

Note: If you perform a fresh install with a vCenter Server, replace the VMCA root certificate before you add ESXi hosts. If you do, VMCA signs the whole chain, and you do not have to generate new certificates.

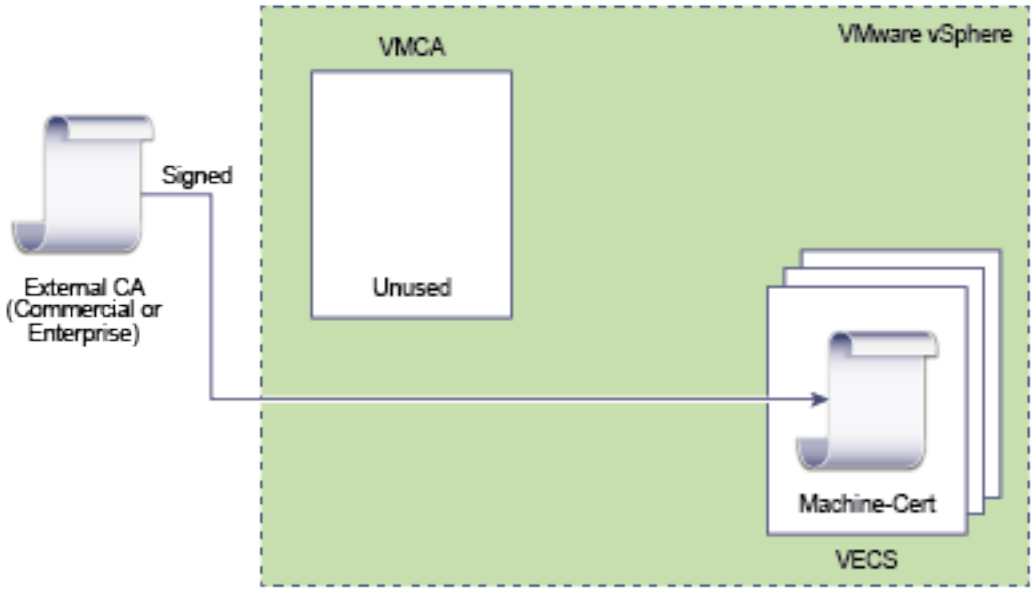
Figure 42: Certificates Signed by a Third-Party or Enterprise CA Use VMCA as an Intermediate CA



Do Not Use VMCA, Provision with Custom Certificates

You can replace the existing VMCA-signed certificates with custom certificates. If you use that approach, you are responsible for all certificate provisioning and monitoring.

Figure 43: External Certificates Are Stored Directly in VECS



Hybrid Deployment

You can have VMCA supply some of the certificates, but use custom certificates for other parts of your infrastructure. For example, because solution user certificates are used only to authenticate to vCenter Single Sign-On, consider having VMCA provision those certificates. Replace the machine SSL certificates with custom certificates to secure all SSL traffic.

Company policy often does not allow intermediate CAs. For those cases, hybrid deployment is a good solution. It minimizes the number of certificates to replace, and secures all traffic. The hybrid deployment leaves only internal traffic, that is, solution user traffic, to use the default VMCA-signed certificates.

ESXi Certificate Replacement

For ESXi hosts, you can change certificate provisioning behavior from the vSphere Client. See the *vSphere Security* documentation for details.

Table 105: ESXi Certificate Replacement Options

Option	Description
VMware Certificate Authority mode (default)	When you renew certificates from the vSphere Client, VMCA issues the certificates for the hosts. If you changed the VMCA root certificate to include a certificate chain, the host certificates include the full chain.
Custom Certificate Authority mode	Allows you to update and use certificates manually that are not signed or issued by VMCA.
Thumbprint mode	Can be used to retain 5.5 certificates during refresh. Use this mode only temporarily in debugging situations.

Where vSphere Uses Certificates

The VMware Certificate Authority (VMCA) provisions your environment with certificates. Certificates include machine SSL certificates for secure connections, solution user certificates for authentication of services to vCenter Single Sign-On, and certificates for ESXi hosts.

The following certificates are in use.

Table 106: Certificates in vSphere

Certificate	Provisioned	Comments
ESXi certificates	VMCA (default)	Stored locally on ESXi host.
Machine SSL certificates	VMCA (default)	Stored in VECS.
Solution user certificates	VMCA (default)	Stored in VECS.
vCenter Single Sign-On SSL signing certificate	Provisioned during installation.	Manage this certificate from the command line. **Note:** Do not change this certificate in the filesystem or unpredictable behavior results.
VMware Directory Service (VMDIR) SSL certificate	Provisioned during installation.	Starting with vSphere 6.5, the machine SSL certificate is used as the vmdir certificate.
SMS self-signed certificates	Provisioned during registration of the IOFilter Provider.	In vSphere 7.0 and later, SMS self-signed certificates are stored in `/etc/vmware/ssl/iofilter vp_castore.pem`. Before vSphere 7.0, SMS self-signed certificates are stored in `/etc/vm ware/ssl/castore.pem`. In addition, the SMS Store can also store VVOL VASA Provider's (version 4.0 and earlier) self-signed certificates when retainVasaProviderCertificate=True.

ESXi

ESXi certificates are stored locally on each host in the `/etc/vmware/ssl` directory. ESXi certificates are provisioned by VMCA by default, but you can use custom certificates instead. ESXi certificates are provisioned when the host is first added to vCenter Server and when the host reconnects.

Machine SSL Certificates

The machine SSL certificate for each node is used to create an SSL socket on the server side. SSL clients connect to the SSL socket. The certificate is used for server verification and for secure communication such as HTTPS or LDAPS.

Each vCenter Server node has its own machine SSL certificate. All services that are running on a vCenter Server node use the machine SSL certificate to expose their SSL endpoints.

The following services use the machine SSL certificate.

- The reverse proxy service. SSL connections to individual vCenter services always go to the reverse proxy. Traffic does not go to the services themselves.
- The vCenter Server service (vpxd).
- The VMware Directory Service (vmdir).

VMware products use standard X.509 version 3 (X.509v3) certificates to encrypt session information. Session information is sent over SSL between components.

Solution User Certificates

A solution user encapsulates one or more vCenter Server services. Each solution user must be authenticated to vCenter Single Sign-On. Solution users use certificates to authenticate to vCenter Single Sign-On through SAML token exchange.

A solution user presents the certificate to vCenter Single Sign-On when it first has to authenticate, after a reboot, and after a timeout has elapsed. The timeout (Holder-of-Key Timeout) can be set from the vSphere Client and defaults to 2592000 seconds (30 days).

For example, the vpxd solution user presents its certificate to vCenter Single Sign-On when it connects to vCenter Single Sign-On. The vpxd solution user receives a SAML token from vCenter Single Sign-On and can then use that token to authenticate to other solution users and services.

The following solution user certificate stores are included in VECS:

- `machine` : Used by the license server and the logging service.
  Note: The machine solution user certificate has nothing to do with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine.
- `vpxd` : vCenter service daemon (vpxd) store. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On.
- `vpxd-extension` : vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users.
- `vsphere-webclient` : vSphere Client store. Also includes some additional services such as the performance chart service.
- `wcp` : VMware vSphere® with VMware Tanzu™ store. Also used for vSphere Cluster Services.

Internal Certificates

vCenter Single Sign-On certificates are not stored in VECS and are not managed with certificate management tools. As a rule, changes are not necessary, but in special situations, you can replace these certificates.

vCenter Single Sign-On Signing Certificate	The vCenter Single Sign-On service includes an identity provider service which issues SAML tokens that are used for authentication

	throughout vSphere. A SAML token represents the user's identity, and also contains group membership information. When vCenter Single Sign-On issues SAML tokens, it signs each token with its signing certificate so that clients of vCenter Single Sign-On can verify that the SAML token comes from a trusted source. You can replace this certificate from the CLI. See Replace a vCenter Server STS Certificate Using the Command Line.
VMware Directory Service SSL Certificate	Starting with vSphere 6.5, the machine SSL certificate is used as the VMware directory certificate. For earlier versions of vSphere, see the corresponding documentation.
vSphere Virtual Machine Encryption Certificates	The vSphere Virtual Machine Encryption solution connects with an external Key Management Server (KMS). Depending on how the solution authenticates to the KMS, it might generate certificates and store them in VECS. See the *vSphere Security* documentation.

VMCA and VMware Core Identity Services

Core identity services are part of every vCenter Server system. VMCA is part of every VMware core identity services group. Use the management CLIs and the vSphere Client to interact with these services.

VMware core identity services include several components.

Table 107: Core Identity Services

Service	Description
VMware Directory Service (vmdir)	Identity source that handles SAML certificate management for authentication with vCenter Single Sign-On.
VMware Certificate Authority (VMCA)	Issues certificates for VMware solution users, machine certificates for machines on which services are running, and ESXi host certificates. VMCA can be used as is, or as an intermediary certificate authority. VMCA issues certificates only to clients that can authenticate to vCenter Single Sign-On in the same domain.
VMware Authentication Framework Daemon (VMAFD)	Includes the VMware Endpoint Certificate Store (VECS) and several other authentication services. VMware administrators interact with VECS. The other services are used internally.

VMware Endpoint Certificate Store Overview

VMware Endpoint Certificate Store (VECS) serves as a local (client-side) repository for certificates, private keys, and other certificate information that can be stored in a keystore. You can decide not to use VMCA as your certificate authority and certificate signer, but you must use VECS to store all vCenter certificates, keys, and so on. ESXi certificates are stored locally on each host and not in VECS.

VECS runs as part of the VMware Authentication Framework Daemon (VMAFD). VECS runs on every vCenter Server node, and holds the keystores that contain the certificates and keys.

VECS polls VMware Directory Service (vmdir) periodically for updates to the trusted root store. You can also explicitly manage certificates and keys in VECS using `vecs-cli` commands. See vecs-cli Command Reference.

VECS includes the following stores.

Table 108: Stores in VECS

Store	Description
Machine SSL store (MACHINE_SSL_CERT)	• Used by the reverse proxy service on every vSphere node. • Used by the VMware Directory Service (vmdir) on each vCenter Server node. All services in vSphere 6.0 and later communicate through a reverse proxy, which uses the machine SSL certificate. For backward compatibility, the 5.x services still use specific ports. As a result, some services such as vpxd still have their own port open.
Solution user stores • `machine` • `vpxd` • `vpxd-extension` • `vsphere-webclient` • `wcp`	VECS includes one store for each solution user. The subject of each solution user certificate must be unique, for example, the machine certificate cannot have the same subject as the vpxd certificate. Solution user certificates are used for authentication with vCenter Single Sign-On. vCenter Single Sign-On checks that the certificate is valid, but does not check other certificate attributes. The following solution user certificate stores are included in VECS: • `machine` : Used by the license server and the logging service. **Note:** The machine solution user certificate has nothing to do with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine. • `vpxd` : vCenter service daemon (vpxd) store. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On. • `vpxd-extension` : vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users. • `vsphere-webclient` : vSphere Client store. Also includes some additional services such as the performance chart service. • `wcp` : VMware vSphere® with VMware Tanzu™ store. Also used for vSphere Cluster Services. Each vCenter Server node includes a `machine` certificate.
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.
vSphere Certificate Manager Utility backup store (BACKUP_STORE)	Used by VMCA (VMware Certificate Manager) to support certificate revert. Only the most recent state is stored as a backup, you cannot go back more than one step.
Other stores	Other stores might be added by solutions. For example, the Virtual Volumes solution adds an SMS store. Do not modify the certificates in those stores unless VMware documentation or a VMware Knowledge Base article instructs you to do so. **Note:** Deleting the TRUSTED_ROOTS_CRLS store can damage your certificate infrastructure. Do not delete or modify the TRUSTED_ROOTS_CRLS store.

The vCenter Single Sign-On service stores the token signing certificate and its SSL certificate on disk. You can change the token signing certificate from the CLI.

Some certificates are stored on the file system, either temporarily during startup or permanently. Do not change the certificates on the file system.

Note: Do not change any certificate files on disk unless instructed by VMware documentation or Knowledge Base Articles. Unpredictable behavior might result otherwise.

Managing Certificate Revocation

If you suspect that one of your certificates has been compromised, replace all existing certificates, including the VMCA root certificate.

vSphere supports replacing certificates but does not enforce certificate revocation for ESXi hosts or for vCenter Server systems.

Remove revoked certificates from all nodes. If you do not remove revoked certificates, a man-in-the-middle attack might enable compromise through impersonation with the account's credentials.

Certificate Replacement in Large Deployments

When replacing certificates in deployments with large numbers of vCenter Server hosts, you can use the vSphere Certificate Management utility or replace certificates manually. Some best practices guide the process you choose.

Replacement of Machine SSL Certificates in Environments with Multiple vCenter Server Nodes

If your environment includes multiple vCenter Server nodes, you can replace certificates with the vSphere Client or the vSphere Certificate Manager utility, or manually with ESXCLI commands.

vSphere Certificate Manager	You run vSphere Certificate Manager on each machine. Depending on the task you perform, you are also prompted for certificate information.
Manual Certificate Replacement	For manual certificate replacement, you run the certificate replacement commands on each machine. See the following topics for details: • Replace Machine SSL Certificates with VMCA-Signed Certificates • Replace Machine SSL Certificates (Intermediate CA) • Replace Machine SSL Certificates with Custom Certificates

Replacement of Solution User Certificates in Environments with Multiple vCenter Server Systems in Enhanced Linked Mode

If your environment includes multiple vCenter Server systems in enhanced linked mode, follow these steps for certificate replacement.

Note: When you list solution user certificates in large deployments, the output of `/usr/lib/vmware-vmafd/bin/dir-cli list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

vSphere Certificate Manager	You run vSphere Certificate Manager on each machine. Depending on the task you perform, you are also prompted for certificate information.
Manual Certificate Replacement	1. Generate or request a certificate. You need the following certificates: – A certificate for the machine solution user on each vCenter Server.

  - A certificate for each of the following solution users on each node:
    - `vpxd` solution user
    - `vpxd-extension` solution user
    - `vsphere-webclient` solution user
    - `wcp` solution user
2. Replace the certificates on each node. The precise process depends on the type of certificate replacement that you are performing. See Managing Certificates with the vSphere Certificate Manager Utility.

See the following topics for details:

- Replace Solution User Certificates with New VMCA-Signed Certificates
- Replace Solution User Certificates (Intermediate CA)
- Replace Solution User Certificates with Custom Certificates

Certificate Replacement in Environments That Include External Solutions

Some solutions, such as VMware vCenter Site Recovery Manager or VMware vSphere Replication, are always installed on a different machine than the vCenter Server system. If you replace the default machine SSL certificate on the vCenter Server system, a connection error results if the solution attempts to connect to the vCenter Server system.

You can run the `ls_update_certs` script to resolve the issue. See the VMware knowledge base article at http://kb.vmware.com/kb/2109074 for details.

Managing Certificates with the vSphere Client

You can view and manage certificates by using the vSphere Client. You also can perform many certificate management tasks with the vSphere Certificate Manager utility.

The vSphere Client enables you to perform these management tasks.

- View the machine SSL, Trusted Root, and Security Token Service (STS) certificates.
- Add new Trusted Root certificates, and renew or replace existing machine SSL and STS certificates.
- Generate a custom Certificate Signing Request (CSR) for a machine SSL certificate and replace the certificate when the Certificate Authority returns it.

Most parts of the certificate replacement workflows are supported fully from the vSphere Client. For generating CSRs for machine SSL certificates, you can use either the vSphere Client or the Certificate Manage utility.

Supported Workflows

After you install a vCenter Server, the VMware Certificate Authority on that node provisions all other nodes in the environment with certificates by default. See vSphere Security Certificates for the current recommendations for managing certificates.

You can use one of the following workflows to renew or replace certificates.

Renew Certificates	You can have the VMCA renew machine SSL, solution user, and STS certificates in your environment from the vSphere Client.
Make VMCA an Intermediate CA	You can generate a CSR using the vSphere Certificate Manager utility. You can then edit the certificate you receive from the CSR to add the VMCA to the chain, and then add the certificate chain and private key to your environment. When you then renew all

	certificates, the VMCA provisions all machines and solution users with certificates that the full chain has signed.
Replace Certificates with Custom Certificates	If you do not want to use the VMCA, you can generate CSRs for the certificates that you want to replace. The CA returns a root certificate and a signed certificate for each CSR. You can upload the root certificate and the custom certificates from the vCenter Server.

Note: If you use the VMCA as an intermediate CA, or use custom certificates, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

Explore Certificate Stores from the vSphere Client

A VMware Endpoint Certificate Store (VECS) instance is included on each vCenter Server node. You can explore the different stores inside the VMware Endpoint Certificate Store from the vSphere Client, including machine SSL and trusted root certificates.

For most management tasks, you must have the password for the administrator for the local domain account, administrator@vsphere.local or a different domain if you changed the domain during installation.

See VMware Endpoint Certificate Store Overview for details on the different stores inside VECS.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@`mydomain`.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Explore the certificates stored inside the VMware Endpoint Certificate Store (VECS).

   VMware Endpoint Certificate Store Overview explains what is in the individual stores.
6. To view details for a certificate, select the certificate and click **View Details**.
7. Use the **Actions** menu to renew or replace certificates.

   For example, if you replace the existing certificate, you can later remove the old root certificate. Remove certificates only if you are sure that they are no longer in use.

Set the Threshold for vCenter Certificate Expiration Warnings

vCenter Server monitors all certificates in the VMware Endpoint Certificate Store (VECS) and issues an alarm when a certificate is 30 days or less from its expiration. You can change how soon you are warned with the vpxd.cert.threshold advanced option.

1. Log in to the vSphere Client.
2. Select the vCenter Server object and click **Configure**.
3. Click **Advanced Settings**.
4. Click **Edit Settings** and filter for `threshold`.
5. Change the setting of vpxd.cert.threshold to the desired value and click **Save**.

Renew VMCA Certificates with New VMCA-Signed Certificates from the vSphere Client

You can replace all VMCA-signed certificates with new VMCA-signed certificates. This process is called renewing certificates. You can renew selected certificates or all certificates in your environment from the vSphere Client.

For certificate management, you have to supply the password of the administrator of the local domain (administrator@vsphere.local by default). If you are renewing certificates for a vCenter Server system, you also have to supply the vCenter Single Sign-On credentials for a user with administrator privileges on the vCenter Server system.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*`mydomain`*.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Renew the VMCA-signed machine SSL certificate for the local system.
   a) Select **Machine SSL Certificate**.
   b) Click **Actions** > **Renew**.
   c) Click **Renew**.

      vCenter Server services restart automatically. You must log back in because restarting the services ends the UI session.

Set Up Your System to Use Custom Certificates

You can set up your environment to use custom certificates.

You can generate Certificate Signing Requests (CSRs) for each machine and for each solution user using the Certificate Manager utility. You can also generate CSRs for each machine, and replace certificates when you receive them from the third-party CA, using the vSphere Client. When you submit the CSRs to your internal or third-party CA, the CA returns signed certificates and the root certificate. You can upload both the root certificate and the signed certificates from the vCenter Server UI.

Generate Certificate Signing Request for Machine SSL Certificate Using the vSphere Client (Custom Certificates)

The machine SSL certificate is used by the reverse proxy service on every vCenter Server node. Each machine must have a machine SSL certificate for secure communication with other services. You can use the vSphere Client to generate a Certificate Signing Request (CSR) for the machine SSL certificate and to replace the certificate once it is ready.

The certificate must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- CRT format
- x509 version 3
- SubjectAltName must contain DNS Name=<machine_FQDN>.
- Contains the following Key Usages: Digital Signature, Key Encipherment

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@`mydomain`.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. Enter the credentials of your vCenter Server.
5. Generate the CSR.
   a) For the certificate that you want to replace, under **Machine SSL Certificate**, click **Actions** > **Generate Certificate Signing Request (CSR)**.
   b) Enter your certificate information and click **Next**.

      Note: When you use vCenter Server to generate a CSR with a key size of 16384 bits, the generation takes a few minutes to complete because of the CPU-intensive nature of the operation.
   c) Copy or download the CSR.
   d) Click **Finish**.
   e) Provide the CSR to your Certificate Authority.

When the Certificate Authority returns the certificate, replace the existing certificate in the certificate store. See Add Custom Certificates.

Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates)

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs) that you can then use with your enterprise CA or send to an external certificate authority. You can use the certificates with the different supported certificate replacement processes.

vSphere Certificate Manager prompts you for information. The prompts depend on your environment and on the type of certificate you want to replace.

- For any CSR generation, you are prompted for the password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.

- You are prompted for the host name or IP address of the vCenter Server.
- To generate a CSR for a machine SSL certificate, you are prompted for certificate properties, which are stored in the `certool.cfg` file. For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.

You can run the Certificate Manager tool from the command line as follows:

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

1. On each machine in your environment, start vSphere Certificate Manager and select option 1.
2. Supply the password and the vCenter Server IP address or host name if prompted.
3. Select option 1 to generate the CSR, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.
4. If you also want to replace all solution user certificates, restart Certificate Manager.
5. Select option 5.
6. Supply the password and the vCenter Server IP address or host name if prompted.
7. Select option 1 to generate the CSRs, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.

Perform certificate replacement.

Add a Trusted Root Certificate to the Certificate Store

If you want to use third-party certificates in your environment, you must add a trusted root certificate to the certificate store.

Obtain the custom root certificate from your third-party or in-house CA.

vSphere accepts only valid CA certificates for import. To be valid, a CA certificate must have the CA bit and the keyCertSign bit set in the basic constraint and the key usage X.509 v3 certificate extensions respectively. This implies that the certificate is a CA and its purpose is for certificate signing. See https://www.rfc-editor.org/rfc/rfc5280 for more information.

Ensure that the keyCertSign bit is set for all the certificates in the chain.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under **Trusted Root Certificates**, click **Add**.
6. Click **Browse** and select the location of the certificate chain.

   You can use a file of type CER, PEM, or CRT.
7. Click **Add**.

   The certificate is added to the store.

Add Custom Certificates

You can add custom Machine SSL certificates to the certificate store.

Generate certificate signing requests (CSRs) for each certificate that you want to replace. You can generate the CSRs with the Certificate Manager utility. You can also generate a CSR for a machine SSL certificate using the vSphere Client. Place the certificate and private key in a location that the vCenter Server can access.

Usually, replacing the machine SSL certificate for each component is sufficient.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under **Machine SSL Certificate**, for the certificate that you want to replace, click **Actions** > **Import and Replace Certificate**.
6. Click the appropriate certificate replacement option and click **Next**.

Option	Description
Replace with VMCA	Creates a VMCA-generated CSR to replace the current certificate.
Replace with certificate generated from vCenter Server	Use a certificate signed using a vCenter Server generated CSR to replace the current certificate.
Replace with external CA certificate (requires private key)	Use a certificate signed by an external CA to replace the current certificate.

7. Enter the CSR information, or upload the appropriate certificates.
8. Click **Replace**.

   vCenter Server services restart automatically.

Managing Certificates with the vSphere Certificate Manager Utility

The vSphere Certificate Manager utility allows you to perform most certificate management tasks interactively from the command line. vSphere Certificate Manager prompts you for the task to perform, for certificate locations and other information as needed, and then stops and starts services and replaces certificates for you.

If you use vSphere Certificate Manager, you are not responsible for placing the certificates in VECS (VMware Endpoint Certificate Store) and you are not responsible for starting and stopping services.

Before you run vSphere Certificate Manager, be sure that you understand the replacement process and procure the certificates that you want to use.

CAUTION: vSphere Certificate Manager supports one level of revert. If you run vSphere Certificate Manager twice and notice that you unintentionally corrupted your environment, the tool cannot revert the first of the two runs.

Certificate Manager Utility Location

You can run the tool on the command line as follows:

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Certificate Manager Options and the Workflows in This Document

You run Certificate Manager options in sequence to complete a workflow. Several options, for example, generating CSRs, are used in different workflows.

Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates.

This single-option workflow (Option 2) can be used by itself, or in the intermediate certificate workflow. See Regenerate a New VMCA Root Certificate and Replace All Certificates.

Make VMCA an Intermediate Certificate Authority

To make VMCA an intermediate CA, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing both machine SSL certificates and solution user certificates.

1. To generate a CSR, select Option 2, Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates. You might have to provide some information about the certificate next. When prompted for an option again, select Option 1.
   Submit the CSR to your external or enterprise CA. You receive a signed certificate and a root certificate from the CA.
2. Combine the VMCA root certificate with the CA root certificate and save the file.
3. Select Option 2, Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates. This process replaces all certificates on the local machine.
4. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must replace certificates on each node.
   a. First you replace the machine SSL certificate with the (new) VMCA certificate (Option 3)
   b. Then you replace the solution user certificates with the (new) VMCA certificate (Option 6).

See Make VMCA an Intermediate Certificate Authority (Certificate Manager).

Replacing All Certificate with Custom Certificates

To replace all certificates with custom certificates, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing both machine SSL certificates and solution user certificates.

1. You generate certificate signing requests for the machine SSL certificate and the solution user certificates separately on each machine.
   a. To generate CSRs for the machine SSL certificate, you select Option 1.
   b. If company policy requires that you replace all certificates, you also select Option 5.
2. After you received the signed certificates and the root certificate from your CA, you replace the machine SSL certificate on each machine by using Option 1.
3. If you also want to replace the solution user certificates, you select Option 5.
4. Finally, when multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must repeat the process on each node.

See Replace All Certificates with Custom Certificate (Certificate Manager).

Note: The following prompt appears when you run the Certificate Manager utility:

```
Enter proper value for VMCA 'Name':
```

Respond to the prompt by entering the fully qualified domain name of the machine on which the certificate configuration is running.

Regenerate a New VMCA Root Certificate and Replace All Certificates

You can regenerate the VMCA root certificate, and replace the local machine SSL certificate and the local solution user certificates with VMCA-signed certificates. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must replace certificates on each vCenter Server.

You must know the following information when you run vSphere Certificate Manager with this option.

- Password for administrator@vsphere.local.
- The FQDN of the machine for which you want to generate a new VMCA-signed certificate. All other properties default to the predefined values but can be changed.

When you replace the existing machine SSL certificate with a new VMCA-signed certificate, vSphere Certificate Manager prompts you for information and enters all values, except for the password and the IP address of the vCenter Server, into the `certool.cfg` file.

- Password for administrator@vsphere.local
- Two-letter country code
- Company name
- Organization name
- Organization unit
- State
- Locality
- IP address (optional)
- Email
- Host name, that is, the fully qualified domain name of the machine for which you want to replace the certificate. If the host name does not match the FQDN, certificate replacement does not complete correctly and your environment might end up in an unstable state.
- IP address of vCenter Server.
- VMCA name, that is, the fully qualified domain name of the machine on which the certificate configuration is running.

Note: As of vSphere 7.0 Update 3o, the OU (organizationalUnitName) field is no longer mandatory.

1. Log in to the vCenter Server and start the vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

2. Select option 4, Regenerate a new VMCA Root Certificate and replace all certificates.
3. Respond to the prompts.

   Certificate Manager generates a new VMCA root certificate based on your input and replaces all certificates on the system where you are running Certificate Manager. The replacement process is complete after Certificate Manager has restarted the services.

4. To replace the machine SSL certificate, run vSphere Certificate Manager with option 3, Replace Machine SSL certificate with VMCA Certificate.
5. To replace the solution user certificates, run Certificate Manager with option 6, Replace Solution user certificates with VMCA certificates.

Make VMCA an Intermediate Certificate Authority (Certificate Manager)

You can make VMCA an Intermediate CA by following the prompts from Certificate Manager utility. After you complete the process, VMCA signs all new certificates with the full chain. If you want, you can use Certificate Manager to replace all existing certificates with new VMCA-signed certificates.

VMware does not recommend operating VMCA as a subordinate (or intermediate) certificate authority. If you choose this option, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

To make VMCA an intermediate CA, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing machine SSL certificates.

1. To generate a CSR, select Option 1, Replace Machine SSL certificate with Custom Certificate then Option 1. You receive a signed certificate and a root certificate from the CA.
2. Combine the VMCA root certificate with the CA root certificate and save the file.
3. Select Option 2, Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates. This process replaces all certificates on the local machine.

Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA)

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs). Submit those CSRs to your enterprise CA or to an external certificate authority for signing. You can use the signed certificates with the different supported certificate replacement processes.

vSphere Certificate Manager prompts you for information. The prompts depend on your environment and on the type of certificate that you want to replace.

For any CSR generation, you are prompted for the password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.

- You can use vSphere Certificate Manager to create the CSR.
- If you prefer to create the CSR manually, the certificate that you send to be signed must meet the following requirements.
  - Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
  - PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
  - x509 version 3
  - The CA extension must be set to true for root certificates, and cert sign must be in the list of requirements. For example:

```
basicConstraints        = critical,CA:true
```

```
keyUsage                = critical,digitalSignature,keyCertSign
```

- CRL signing must be enabled.
- Extended Key Usage can be either empty or contain Server Authentication.
- No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is 10 certificates.
- Certificates with wildcards or with more than one DNS name are not supported.
- You cannot create subsidiary CAs of VMCA.
  See the VMware knowledge base article at http://kb.vmware.com/kb/2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x, for an example using Microsoft Certificate Authority.

1. Run the vSphere Certificate Manager.
   `/usr/lib/vmware-vmca/bin/certificate-manager`
2. Select Option 2.
   Initially, you use this option to generate the CSR, not to replace certificates.
3. Supply the password and the vCenter Server IP address or host name if prompted.
4. Select Option 1 to generate the CSR and answer the prompts.
   As part of the process, you have to provide a directory. Certificate Manager places the certificate to be signed (`*.csr` file) and the corresponding key file (`*.key` file) in the directory.
5. Name the certificate signing request (CSR) `root_signing_cert.csr`.
6. Send the CSR to your enterprise or external CA for signing and name the resulting signed certificate `root_signing_cert.cer`.
7. In a text editor, combine the certificates as follows.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8. Save the file as `root_signing_chain.cer`.

Replace the existing root certificate with the chained root certificate. See Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates.

Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates

You can use vSphere Certificate Manager to generate a CSR and send the CSR to an enterprise or third-party CA for signing. You can then replace the VMCA root certificate with a custom signing certificate and replace all existing certificates with certificates that are signed by the custom CA.

- Generate the certificate chain.
  - You can use vSphere Certificate Manager to create the CSR or create the CSR manually.
  - After you receive the signed certificate from your third-party or enterprise CA, combine it with the initial VMCA root certificate to create the full chain.
    See Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA) for certificate requirements and the process of combining the certificates.

- Gather the information that you need.
  - Password for administrator@vsphere.local
  - Valid custom certificate for Root (`.crt` file)
  - Valid custom key for Root (`.key` file)

You run vSphere Certificate Manager on vCenter Server to replace the VMCA root certificate with a custom signing certificate.

1. Start vSphere Certificate Manager on the vCenter Server host and select option 2.
2. Select option 2 again to start certificate replacement and respond to the prompts.
   a) Specify the full path to the root certificate when prompted.
   b) If you are replacing certificates for the first time, you are prompted for information to be used for the machine SSL certificate.

      This information includes the required FQDN of the machine and is stored in the `certool.cfg` file.

Replace Machine SSL Certificate with VMCA Certificate (Intermediate CA)

When you use VMCA as an intermediate CA, you can replace the machine SSL certificate explicitly. First you replace the VMCA root certificate on the vCenter Server, then you can replace the machine SSL certificate, which will be signed by the VMCA's new root. You can also use this option to replace machine SSL certificates that are corrupt or about to expire.

- You must know the following information to run Certificate Manager with this option.
  – Password for administrator@vsphere.local.
  – The FQDN of the machine for which you want to generate a new VMCA-signed certificate. All other properties default to the predefined values but can be changed.
  – Host name or IP address of the vCenter Server system.

When you replace the existing machine SSL certificate with a new VMCA-signed certificate, vSphere Certificate Manager prompts you for information and enters all values, except for the password and the IP address of the vCenter Server, into the `certool.cfg` file.

- Password for administrator@vsphere.local
- Two-letter country code
- Company name
- Organization name
- Organization unit
- State
- Locality
- IP address (optional)
- Email
- Host name, that is, the fully qualified domain name of the machine for which you want to replace the certificate. If the host name does not match the FQDN, certificate replacement does not complete correctly and your environment might end up in an unstable state.
- IP address of vCenter Server.
- VMCA name, that is, the fully qualified domain name of the machine on which the certificate configuration is running.

Note: As of vSphere 7.0 Update 3o, the OU (organizationalUnitName) field is no longer mandatory.

1. Start vSphere Certificate Manager and select option 3.
2. Respond to the prompts.

   Certificate Manager stores the information in the `certool.cfg` file.

vSphere Certificate Manager replaces the machine SSL certificate.

Replace Solution User Certificates with VMCA Certificates (Intermediate CA)

When you use VMCA as an intermediate CA, you can replace the solution user certificate explicitly. First you replace the VMCA root certificate on the vCenter Server, then you can replace the solution user certificate, which will be signed by the VMCA's new root. You can also use this option to replace solution certificates that are corrupt or about to expire.

- Restart all vCenter Server nodes explicitly if you replaced the VMCA root certificate in a deployment consisting of multiple instances of vCenter Server in Enhanced Linked Mode configuration.
- You must know the following information to run Certificate Manager with this option.
  - Password for administrator@vsphere.local
  - Host name or IP address of the vCenter Server system

1. Start vSphere Certificate Manager and select option 6.
2. Respond to the prompts.

   See the VMware knowledge base article at http://kb.vmware.com/kb/2112281 for more information.

vSphere Certificate Manager replaces all solution user certificates.

Replace All Certificates with Custom Certificate (Certificate Manager)

You can use the vSphere Certificate Manager utility to replace all certificates with custom certificates. Before you start the process, you must send CSRs to your CA. You can use Certificate Manager to generate the CSRs.

One option is to replace only the machine SSL certificate, and to use the solution user certificates that are provisioned by VMCA. Solution user certificates are used only for communication between vSphere components.

When you use custom certificates, you replace the VMCA-signed certificates with custom certificates. You can use the vSphere Client, the vSphere Certificate Manager utility, or CLIs for manual certificate replacement. Certificates are stored in VECS.

To replace all certificates with custom certificates, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing both machine SSL certificates and solution user certificates.

1. You generate certificate signing requests for the machine SSL certificate and the solution user certificates separately on each machine.
   a. To generate CSRs for the machine SSL certificate, you select Option 1.
   b. If company policy does not allow a hybrid deployment, you select Option 5.
2. After you received the signed certificates and the root certificate from your CA, you replace the machine SSL certificate on each machine by using Option 1.
3. If you also want to replace the solution user certificates, you select Option 5.
4. Finally, when multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you have to repeat the process on each node.

Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates)

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs) that you can then use with your enterprise CA or send to an external certificate authority. You can use the certificates with the different supported certificate replacement processes.

vSphere Certificate Manager prompts you for information. The prompts depend on your environment and on the type of certificate you want to replace.

- For any CSR generation, you are prompted for the password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.

- You are prompted for the host name or IP address of the vCenter Server.
- To generate a CSR for a machine SSL certificate, you are prompted for certificate properties, which are stored in the `certool.cfg` file. For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.

You can run the Certificate Manager tool from the command line as follows:

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

1. On each machine in your environment, start vSphere Certificate Manager and select option 1.
2. Supply the password and the vCenter Server IP address or host name if prompted.
3. Select option 1 to generate the CSR, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.
4. If you also want to replace all solution user certificates, restart Certificate Manager.
5. Select option 5.
6. Supply the password and the vCenter Server IP address or host name if prompted.
7. Select option 1 to generate the CSRs, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.

Perform certificate replacement.

Replace Machine SSL Certificate with Custom Certificate

The machine SSL certificate is used by the reverse proxy service on every vCenter Server node. Each machine must have a machine SSL certificate for secure communication with other services. You can replace the certificate on each node with a custom certificate.

Before you start, you need a CSR for each machine in your environment. You can generate the CSR using vSphere Certificate Manager or explicitly.

1. To generate the CSR using vSphere Certificate Manager, see Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates).
2. To generate the CSR explicitly, request a certificate for each machine from your third-party or enterprise CA. The certificate must meet the following requirements:
   - Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
   - CRT format
   - x509 version 3
   - SubjectAltName must contain DNS Name=<machine_FQDN>.
   - Contains the following Key Usages: Digital Signature, Key Encipherment

See also the VMware knowledge base article at http://kb.vmware.com/kb/2112014, Obtaining vSphere certificates from a Microsoft Certificate Authority.

1. Start vSphere Certificate Manager and select option 1.
2. Select option 2 to start certificate replacement and respond to the prompts.

   vSphere Certificate Manager prompts you for the following information:

   - Password for administrator@vsphere.local
   - Valid Machine SSL custom certificate (`.crt` file)
   - Valid Machine SSL custom key (`.key` file)
   - Valid signing certificate for the custom machine SSL certificate (`.crt` file)
   - IP address of the vCenter Server

Replace Solution User Certificates with Custom Certificates

Many companies only require that you replace certificates of services that are accessible externally. However, Certificate Manager also supports replacing solution user certificates. Solution users are collections of services, for example, all services that are associated with the vSphere Client.

Before you start, you need a CSR for each machine in your environment. You can generate the CSR using vSphere Certificate Manager or explicitly.

1. To generate the CSR using vSphere Certificate Manager, see Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates).
2. Request a certificate for each solution user on each node from your third-party or enterprise CA. You can generate the CSR using vSphere Certificate Manager or prepare it yourself. The CSR must meet the following requirements:
   - Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
   - CRT format
   - x509 version 3
   - SubjectAltName must contain DNS Name=<machine_FQDN>.
   - Each solution user certificate must have a different `Subject`. Consider, for example, including the solution user name (such as vpxd) or other unique identifier.
   - Contains the following Key Usages: Digital Signature, Key Encipherment

See also the VMware knowledge base article at http://kb.vmware.com/kb/2112014, Obtaining vSphere certificates from a Microsoft Certificate Authority.

When you are prompted for a solution user certificate, provide the complete signing certificate chain of the third-party CA.

The format looks similar to the following.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
```

```
-----END CERTIFICATE-----
```

1. Start vSphere Certificate Manager and select option 5.
2. Select option 2 to start certificate replacement and respond to the prompts.
   vSphere Certificate Manager prompts you for the following information:
   - Password for administrator@vsphere.local
   - Certificate and key for machine solution user
   - The certificate and key (`vpxd.crt` and `vpxd.key`) for the machine solution user
   - The full set of certificates and keys (`vpxd.crt` and `vpxd.key`) for all solution users

Revert Last Performed Operation by Republishing Old Certificates

When you perform a certificate management operation by using vSphere Certificate Manager, the current certificate state is stored in the BACKUP_STORE store in VECS before certificates are replaced. You can revert the last performed operation and return to the previous state.

Note: The revert operation restores what is currently in the BACKUP_STORE. If you run vSphere Certificate Manager with two different options and you then attempt to revert, only the last operation is reverted.

Reset All Certificates Using the Certificate Manager

You can use the vSphere Certificate Manager utility to replace all existing vCenter certificates with certificates that are signed by VMCA.

When you use this option, you overwrite all custom certificates that are currently in VMware Endpoint Certificate Store (VECS).
vSphere Certificate Manager can replace all certificates. Which certificates are replaced depends on which options you select.

1. Log in to vCenter Server shell and start the vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

2. Select Option 8, Reset all Certificates.
3. Enter the administrator user and password.
4. When prompted, enter your certificate information.

After certificates are replaced and services are restarted, verify your certificate information.

Manual Certificate Replacement

For some special certificate replacement cases, you cannot use the vSphere Certificate Manager utility. Instead, you can use the CLIs included with your installation for certificate replacement.

Understanding Stopping and Starting of Services

For certain parts of manual certificate replacement, you must stop all services and then start only the services that manage the certificate infrastructure. If you stop services only when needed, you can minimize downtime.

You have to stop and start services as part of the certificate replacement process. You can use the `service-control` command for starting and stopping services. You can start and stop all services or individual services. See the command-line help for more information.

Follow these guidelines.

- Do not stop services to generate new public/private key pairs or new certificates.

- If you are the only administrator, you do not have to stop services when you add a new root certificate. The old root certificate remains available, and all services can still authenticate with that certificate. Stop and immediately restart all services after you add the root certificate to avoid problems with your hosts.
- If your environment includes multiple administrators, stop services before you add a new root certificate and restart services after you add a new certificate.
- Stop services right before you delete a machine SSL certificate in VECS.

Replace Existing VMCA-Signed Certificates with New VMCA-Signed Certificates

If the VMCA root certificate expires in the near future, or if you want to replace it for other reasons, you can generate a new root certificate and add it to the VMware Directory Service. You can then generate new machine SSL certificates and solution user certificates using the new root certificate.

Only administrator@vsphere.local or other users in the CAAdmins group can perform certificate management tasks. See Add Members to a vCenter Single Sign-On Group.

Use the vSphere Certificate Manager utility to replace certificates for most cases.

If you need fine-grained control, this scenario gives detailed step-by-step instructions for replacing the complete set of certificates using CLI commands. You can instead replace only individual certificates using the procedure in the corresponding task.

Generate a New VMCA-Signed Root Certificate

You generate new VMCA-signed certificates with the `certool` CLI or the vSphere Certificate Manager utility and publish the certificates to vmdir.

1. On the vCenter Server, generate a new self-signed certificate and private key.

   ```
   certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config <config_file>
   ```

2. Replace the existing root certificate with the new certificate.

   ```
   certool --rootca --cert <cert_file_path> --privkey <key_file_path>
   ```

   The command generates the certificate, adds it to vmdir, and adds it to VECS.

3. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```

4. Optional: Publish the new root certificate to vmdir.

   ```
   dir-cli trustedcert publish --cert newRoot.crt
   ```

   The command updates all instances of vmdir immediately. If you do not run the command, propagation of the new certificate to all nodes might take a while.

5. Restart all services.

   ```
   service-control --start --all
   ```

Generate a New VMCA-Signed Root Certificate

The following example shows all the steps for verifying the current root CA information, and for regenerating the root certificate.

1. (Optional) On the vCenter Server, list the VMCA root certificate to make sure it is in the certificate store.

   ```
   /usr/lib/vmware-vmca/bin/certool --getrootca
   ```

The output looks similar to this:

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2. (Optional) List the VECS TRUSTED_ROOTS store and compare the certificate serial number there with the output from Step 1.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry list --store TRUSTED_ROOTS --text
   ```

   In the simplest case with only one root certificate, the output looks like this:

   ```
   Number of entries in store :    1
   Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
   Entry type :    Trusted Cert
   Certificate:
       Data:
           Version: 3 (0x2)
           Serial Number:
               cf:2d:ff:49:88:50:e5:af
   ```

3. Generate a new VMCA root certificate. The command adds the certificate to the TRUSTED_ROOTS store in VECS and in vmdir (VMware Directory Service).

   ```
   /usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/cer-
   tool.cfg
   ```

Replace Machine SSL Certificates with VMCA-Signed Certificates

After you generate a new VMCA-signed root certificate, you can replace all machine SSL certificates in your environment.

Be prepared to stop all services and to start the services that handle certificate propagation and storage.

Each machine must have a machine SSL certificate for secure communication with other services. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must run the Machine SSL certificate generation commands on each node.

1. Make one copy of `certool.cfg` for each machine that needs a new certificate.

   You can find the `certool.cfg` file in the `/usr/lib/vmware-vmca/share/config/` directory.

2. Edit the custom configuration file for each machine to include that machine's FQDN.

   Run `NSLookup` against the machine's IP address to see the DNS listing of the name, and use that name for the Hostname field in the file.

3. Generate a public/private key file pair and a certificate for each file, passing in the configuration file that you just customized.

   For example:

   ```
   certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
   certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --config machine1.cfg
   ```

4. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```

5. Add the new certificate to VECS.

   All machines need the new certificate in the local certificate store to communicate over SSL. You first delete the existing entry, then add the new entry.

   ```
   vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
   vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt --key ma-
   chine1.priv
   ```

6. Restart all services.

   ```
   service-control --start --all
   ```

Replacing Machine Certificates with VMCA-Signed Certificates

1. Create a configuration file for the SSL certificate and save it as `ssl-config.cfg` in the current directory.

   ```
   Country = US
   Name = vmca-<FQDN-example>
   Organization = <my_company>
   OrgUnit = <my_company Engineering>
   State = <my_state>
   Locality = <mytown>
   Hostname = <FQDN>
   ```

2. Generate a key pair for the machine SSL certificate. In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, run this command on each vCenter Server node.

   ```
   /usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
   ```

   The `ssl-key.priv` and `ssl-key.pub` files are created in the current directory.

3. Generate the new machine SSL certificate. This certificate is signed by VMCA. If you replaced the VMCA root certificate with custom certificate, VMCA signs all certificates with the full chain.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --
   config=ssl-config.cfg
   ```

   The `new-vmca-ssl.crt` file is created in the current directory.

4. (Optional) List the content of VECS.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli store list
   ```

   – Sample output on vCenter Server:

   ```
   output (on vCenter):
   MACHINE_SSL_CERT
   TRUSTED_ROOTS
   TRUSTED_ROOT_CRLS
   machine
   vsphere-webclient
   vpxd
   vpxd-extension
   hvc
   data-encipherment
   APPLMGMT_PASSWORD
   SMS
   wcp
   KMS_ENCRYPTION
   ```

5. Replace the Machine SSL certificate in VECS with the new Machine SSL certificate. The `--store` and `--alias` values have to exactly match with the default names.

   – On each vCenter Server, run the following commands to update the Machine SSL certificate in the MACHINE_SSL_CERT store. You must update the certificate for each machine separately because each has a different FQDN.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
 __MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
 __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

You can also replace the certificates for your ESXi hosts. See the *vSphere Security* publication.

Replace Solution User Certificates with New VMCA-Signed Certificates

After you replace the machine SSL certificates, you can replace all solution user certificates. Solution user certificates must be valid, that is, not expired, but none of the other information in the certificate is used by the certificate infrastructure.

Be prepared to stop all services and to start the services that handle certificate propagation and storage.

Many VMware customers do not replace solution user certificates. They replace only the machine SSL certificates with custom certificates. This hybrid approach satisfies the requirements of their security teams.

- Certificates either sit behind a proxy, or they are custom certificates.
- No intermediate CAs are used.

You replace the machine solution user certificate and the solution user certificate on each vCenter Server system.

Note: When you list solution user certificates in large deployments, the output of `/usr/lib/vmware-vmafd/bin/dir-cli list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

1. Make one copy of `certool.cfg`, remove the Name, IP address, DNS name, and email fields, and rename the file, for example, to `sol_usr.cfg`.

   You can name the certificates from the command line as part of generation. The other information is not needed for solution users. If you leave the default information, the certificates that are generated are potentially confusing.

2. Generate a public/private key file pair and a certificate for each solution user, passing in the configuration file that you just customized.

   For example:

   ```
   /usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
   /usr/lib/vmware-vmca/bin/certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config
    sol_usr.cfg
   ```

3. Find the name for each solution user.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli service list
   ```

   You can use the unique ID that is returned when you replace the certificates. The input and output might look as follows.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
   4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
   5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
   6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
   ```

   In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, the output of `/usr/lib/vmware-vmafd/bin/dir-cli service list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

4. Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5. For each solution user, replace the existing certificate in vmdir and then in VECS.

   The following example shows how to replace the certificates for the vpxd service.

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

   Note: Solution users cannot authenticate to vCenter Single Sign-On if you do not replace the certificate in vmdir.

6. Restart all services.

```
service-control --start --all
```

Using VMCA-Signed Solution User Certificates

1. Generate a public/private key pair for each solution user on each vCenter Server node in an Enhanced Linked Mode configuration. That includes a pair for the machine solution and a pair for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp).
   a. Generate a key pair for the machine solution user.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=ma-
chine-key.pub
```

   b. Generate a key pair for the vpxd solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

   c. Generate a key pair for the vpxd-extension solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pub-
key=vpxd-extension-key.pub
```

   d. Generate a key pair for the vsphere-webclient solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=v-
sphere-webclient-key.pub
```

   e. Generate a key pair for the wcp solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2. Generate solution user certificates that are signed by the new VMCA root certificate for the machine solution user and for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp) on each vCenter Server node.

   Note: The `--Name` parameter has to be unique. Including the name of the solution user store name makes it easy to see which certificate maps to which solution user. The example includes the name, for example vpxd or vpxd-extension in each case.

   a. Make one copy of the `/usr/lib/vmware-vmca/share/config/certool.cfg` file, then modify or remove the Name, IP address, DNS name, and email fields as required, and rename the file, for example, to `sol_usr.cfg`.

   b. Generate a certificate for the machine solution user on each node.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv
    --Name=machine --config sol_usr.cfg
   ```

   c. Generate a certificate for the vpxd solution user on each node.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --
   Name=vpxd --config sol_usr.cfg
   ```

   d. Generate a certificate for the vpxd-extensions solution user on each node.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-ex-
   tension-key.priv --Name=vpxd-extension --config sol_usr.cfg
   ```

   e. Generate a certificate for the vsphere-webclient solution user on each node by running the following command.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --privkey=v-
   sphere-webclient-key.priv --Name=vsphere-webclient --config sol_usr.cfg
   ```

   f. Generate a certificate for the wcp solution user on each node by running the following command.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
   Name=wcp --config sol_usr.cfg
   ```

3. Replace the solution user certificates in VECS with the new solution user certificates.

   Note: The `--store` and `--alias` parameters have to exactly match the default names for services.

   a. Replace the machine solution user certificate on each node:

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
   /usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert new-
   machine.crt --key machine-key.priv
   ```

   b. Replace the vpxd solution user certificate on each node.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
   /usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
   vpxd.crt --key vpxd-key.priv
   ```

   c. Replace the vpxd-extension solution user certificate on each node.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-exten-
   sion
   /usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-exten-
   sion --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
   ```

   d. Replace the vsphere-webclient solution user certificate on each node.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias vsphere-
   webclient
   /usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias vsphere-
   webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
   ```

   e. Replace the wcp solution user certificate on each node.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
   /usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-wcp.crt
    --key wcp-key.priv
   ```

4. Update VMware Directory Service (vmdir) with the new solution user certificates. You are prompted for a vCenter Single Sign-On administrator password.
   a. Run `/usr/lib/vmware-vmafd/bin/dir-cli service list` to get the unique service ID suffix for each solution user. You run this command on a vCenter Server system.

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service list
      output:
      1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
      2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
      3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
      4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
      5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
      6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
      ```

      Note: When you list solution user certificates in large deployments, the output of `/usr/lib/vmware-vmafd/bin/dir-cli list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.
   b. Replace the machine certificate in vmdir on each vCenter Server node. For example, if machine-6fd7f140-60a9-11e4-9e28-005056895a69 is the machine solution user on the vCenter Server, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name ma-
      chine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
      ```
   c. Replace the vpxd solution user certificate in vmdir on each node. For example, if vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name
       vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
      ```
   d. Replace the vpxd-extension solution user certificate in vmdir on each node. For example, if vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd-extension solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name vpxd-exten-
      sion-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
      ```
   e. Replace the vsphere-webclient solution user certificate on each node. For example, if vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 is the vsphere-webclient solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-webclien-
      t-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
      ```
   f. Replace the wcp solution user certificate on each node. For example, if wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e is the wcp solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
      b5e7-9460e2b8200e --cert new-wcp.crt
      ```

Restart all services on each vCenter Server node.

Use VMCA as an Intermediate Certificate Authority

You can replace the VMCA root certificate with a third-party CA-signed certificate that includes VMCA in the certificate chain. Going forward, all certificates that VMCA generates include the full chain. You can replace existing certificates with newly generated certificates.

If you use VMCA as an intermediate CA, or use custom certificates, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

Replace the Root Certificate (Intermediate CA)

The first step in replacing the VMCA certificates with custom certificates is generating a CSR, and sending the CSR to be signed. You then add the signed certificate to VMCA as a root certificate.

You can use the Certificate Manager utility or other tool to generate the CSR. The CSR must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
- x509 version 3
- The CA extension must be set to true for root certificates, and cert sign must be in the list of requirements. For example:

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- CRL signing must be enabled.
- Extended Key Usage can be either empty or contain Server Authentication.
- No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is 10 certificates.
- Certificates with wildcards or with more than one DNS name are not supported.
- You cannot create subsidiary CAs of VMCA.
  See the VMware knowledge base article at http://kb.vmware.com/kb/2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x, for an example using Microsoft Certificate Authority.

VMCA validates the following certificate attributes when you replace the root certificate:

- Key size: 2048 bits (minimum) to 16384 bits (maximum)
- Key Usage: Cert Sign
- Basic Constraint: Subject Type CA

1. Generate a CSR and send it to your CA.
   Follow your CA's instructions.
2. Prepare a certificate file that includes the signed VMCA certificate and the full CA chain of your third-party CA or enterprise CA. Save the file, for example as `rootca1.crt`.
   You can accomplish this step by copying all CA certificates in PEM format into a single file. You start with the VMCA root certificate and end up with the root CA PEM certificate. For example:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3. Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4. Replace the existing VMCA root CA.

   ```
   certool --rootca --cert=rootca1.crt --privkey=root1.key
   ```

   When you run this command, it:

   - Adds the new custom root certificate to the certificate location in the file system.
   - Appends the custom root certificate to the TRUSTED_ROOTS store in VECS (after a delay).
   - Adds the custom root certificate to vmdir (after a delay).

5. Optional: To propagate the change to all instances of vmdir (VMware Directory Service), publish the new root certificate to vmdir, supplying the full file path for each file.

   For example, if the certificate has only one certificate in the chain:

   ```
   dir-cli trustedcert publish --cert rootca1.crt
   ```

   If the certificate has more than one certificate in the chain:

   ```
   dir-cli trustedcert publish --cert rootca1.crt --chain
   ```

   Replication between vmdir nodes happens every 30 seconds. You do not have to add the root certificate to VECS explicitly because VECS polls vmdir for new root certificate files every 5 minutes.

6. Optional: If necessary, you can force a refresh of VECS.

   ```
   vecs-cli force-refresh
   ```

7. Restart all services.

   ```
   service-control --start --all
   ```

Replacing the Root Certificate

Replace the VMCA root certificate with the custom CA root certificate using the `certool` command with the `--rootca` option.

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/root.key
```

When you run this command, it:

- Adds the new custom root certificate to the certificate location in the file system.
- Appends the custom root certificate to the TRUSTED_ROOTS store in VECS.
- Adds the custom root certificate to vmdir.

You can remove the original VMCA root certificate from the certificate store if your company policy requires it. If you do, you have to replace the vCenter Single Sign-On Signing certificate. See Replace a vCenter Server STS Certificate Using the Command Line.

Replace Machine SSL Certificates (Intermediate CA)

After you have received the signed certificate from the CA and made it the VMCA root certificate, you can replace all machine SSL certificates.

For each machine SSL certificate, the `SubjectAltName` must contain `DNS Name=<Machine FQDN>`.

These steps are essentially the same as the steps for replacing with a certificate that uses VMCA as the certificate authority. However, in this case, VMCA signs all certificates with the full chain.

Each machine must have a machine SSL certificate for secure communication with other services. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must run the Machine SSL certificate generation commands on each node.

1. Make one copy of `certool.cfg` for each machine that needs a new certificate.

   The `certool.cfg` file is located in the `/usr/lib/vmware-vmca/share/config/` directory.

2. Edit the custom configuration file for each machine to include that machine's FQDN.

   Run `NSLookup` against the machine's IP address to see the DNS listing of the name, and use that name for the Hostname field in the file.

3. Generate a public/private key file pair and a certificate for each machine, passing in the configuration file that you just customized.

   For example:

   ```
   certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
   certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --config machine1.cfg
   ```

4. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```

5. Add the new certificate to VECS.

   All machines need the new certificate in the local certificate store to communicate over SSL. You first delete the existing entry, then add the new entry.

   ```
   vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
   vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
   --key machine1.priv
   ```

6. Restart all services.

   ```
   service-control --start --all
   ```

Replacing Machine SSL Certificates (VMCA Is Intermediate CA)

1. Create a configuration file for the SSL certificate and save it as `ssl-config.cfg` in the current directory.

   ```
   Country = US
   Name = vmca-<FQDN-example>
   Organization = VMware
   OrgUnit = VMware Engineering
   State = California
   Locality = Palo Alto
   Hostname = <FQDN>
   ```

2. Generate a key pair for the machine SSL certificate. In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, run this command on each vCenter Server node.

   ```
   /usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
   ```

   The `ssl-key.priv` and `ssl-key.pub` files are created in the current directory.

3. Generate the new machine SSL certificate. This certificate is signed by VMCA. If you replaced the VMCA root certificate with custom certificate, VMCA signs all certificates with the full chain.

   ```
   /usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --
   config=ssl-config.cfg
   ```

   The `new-vmca-ssl.crt` file is created in the current directory.

4. (Optional) List the content of VECS.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli store list
   ```

   – Sample output on vCenter Server:

   ```
   output (on vCenter):
   MACHINE_SSL_CERT
   TRUSTED_ROOTS
   TRUSTED_ROOT_CRLS
   ```

```
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

5. Replace the Machine SSL certificate in VECS with the new Machine SSL certificate. The `--store` and `--alias` values have to exactly match with the default names.
   – On each vCenter Server, run the following commands to update the Machine SSL certificate in the MACHINE_SSL_CERT store. You must update the certificate for each machine separately because each has a different FQDN.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
 __MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
 __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Replace Solution User Certificates (Intermediate CA)

After you replace the machine SSL certificates, you can replace the solution user certificates.

Each solution user certificate must have a different `Subject`. Consider, for example, including the solution user name (such as vpxd) or other unique identifier.

Many VMware customers do not replace solution user certificates. They replace only the machine SSL certificates with custom certificates. This hybrid approach satisfies the requirements of their security teams.

- Certificates either sit behind a proxy, or they are custom certificates.
- No intermediate CAs are used.

You replace the machine solution user certificate and the solution user certificate on each vCenter Server system.

Note: When you list solution user certificates in large deployments, the output of `/usr/lib/vmware-vmafd/bin/dir-cli list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

1. Make one copy of `certool.cfg`, remove the Name, IP address, DNS name, and email fields, and rename the file, for example, to `sol_usr.cfg`.

   You can name the certificates from the command line as part of generation. The other information is not needed for solution users. If you leave the default information, the certificates that are generated are potentially confusing.

2. Generate a public/private key file pair and a certificate for each solution user, passing in the configuration file that you just customized.

   For example:

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3. Find the name for each solution user.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli service list
   ```

   You can use the unique ID that is returned when you replace the certificates. The input and output might look as follows.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
   4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
   5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
   6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
   ```

   In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, the output of `/usr/lib/vmware-vmafd/bin/dir-cli service list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

4. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```

5. Replace the existing certificate in vmdir and then in VECS.

   For solution users, you must add the certificates in that order. For example:

   ```
   dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
   vecs-cli entry delete --store vpxd --alias vpxd
   vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
   ```

   Note: Solution users cannot log in to vCenter Single Sign-On if you do not replace the certificate in vmdir.

6. Restart all services.

   ```
   service-control --start --all
   ```

Replacing Solution User Certificates (Intermediate CA)

1. Generate a public/private key pair for each solution user on each vCenter Server node in an Enhanced Linked Mode configuration. That includes a pair for the machine solution and a pair for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp).
   a. Generate a key pair for the machine solution user.

      ```
      /usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
      ```

   b. Generate a key pair for the vpxd solution user on each node.

      ```
      /usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
      ```

   c. Generate a key pair for the vpxd-extension solution user on each node.

      ```
      /usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
      ```

   d. Generate a key pair for the vsphere-webclient solution user on each node.

      ```
      /usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
      ```

e. Generate a key pair for the wcp solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2. Generate solution user certificates that are signed by the new VMCA root certificate for the machine solution user and for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp) on each vCenter Server node.

   Note: The `--Name` parameter has to be unique. Including the name of the solution user store name makes it easy to see which certificate maps to which solution user. The example includes the name, for example vpxd or vpxd-extension in each case.

   a. Make one copy of the `/usr/lib/vmware-vmca/share/config/certool.cfg` file, then modify or remove the Name, IP address, DNS name, and email fields as required, and rename the file, for example, to `sol_usr.cfg`.

   b. Generate a certificate for the machine solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv
 --Name=machine --config sol_usr.cfg
```

   c. Generate a certificate for the vpxd solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --
Name=vpxd --config sol_usr.cfg
```

   d. Generate a certificate for the vpxd-extensions solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-ex-
tension-key.priv --Name=vpxd-extension --config sol_usr.cfg
```

   e. Generate a certificate for the vsphere-webclient solution user on each node by running the following command.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --privkey=v-
sphere-webclient-key.priv --Name=vsphere-webclient --config sol_usr.cfg
```

   f. Generate a certificate for the wcp solution user on each node by running the following command.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp --config sol_usr.cfg
```

3. Replace the solution user certificates in VECS with the new solution user certificates.

   Note: The `--store` and `--alias` parameters have to exactly match the default names for services.

   a. Replace the machine solution user certificate on each node:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert new-
machine.crt --key machine-key.priv
```

   b. Replace the vpxd solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

   c. Replace the vpxd-extension solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-exten-
sion
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-exten-
sion --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

   d. Replace the vsphere-webclient solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias vsphere-
webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias vsphere-
webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

   e. Replace the wcp solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
```

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-wcp.crt
 --key wcp-key.priv
```

4. Update VMware Directory Service (vmdir) with the new solution user certificates. You are prompted for a vCenter Single Sign-On administrator password.
   a. Run `/usr/lib/vmware-vmafd/bin/dir-cli service list` to get the unique service ID suffix for each solution user. You run this command on a vCenter Server system.

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service list
      output:
      1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
      2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
      3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
      4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
      5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
      6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
      ```

      Note: When you list solution user certificates in large deployments, the output of `/usr/lib/vmware-vmafd/bin/dir-cli list` includes all solution users from all nodes. Run `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.
   b. Replace the machine certificate in vmdir on each vCenter Server node. For example, if machine-6fd7f140-60a9-11e4-9e28-005056895a69 is the machine solution user on the vCenter Server, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name ma-
      chine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
      ```
   c. Replace the vpxd solution user certificate in vmdir on each node. For example, if vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name
       vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
      ```
   d. Replace the vpxd-extension solution user certificate in vmdir on each node. For example, if vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd-extension solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name vpxd-exten-
      sion-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
      ```
   e. Replace the vsphere-webclient solution user certificate on each node. For example, if vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 is the vsphere-webclient solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-webclien-
      t-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
      ```
   f. Replace the wcp solution user certificate on each node. For example, if wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e is the wcp solution user ID, run this command:

      ```
      /usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
      b5e7-9460e2b8200e --cert new-wcp.crt
      ```

Use Custom Certificates with vSphere

If your company policy requires it, you can replace some or all certificates used in vSphere with certificates that are signed by a third-party or enterprise CA. If you do that, VMCA is not in your certificate chain. You are responsible for storing all vCenter certificates in VECS.

You can replace all certificates or use a hybrid solution. For example, consider replacing all certificates that are used for network traffic but leaving VMCA-signed solution user certificates. Solution user certificates are used only for

authentication to vCenter Single Sign-On. vCenter Server uses solution user certificates for internal communication only. Solution user certificates are not used for external communication.

Note: If you do not want to use VMCA, you are responsible for replacing all certificates yourself, for provisioning new components with certificates, and for tracking certificate expiration.

Even if you decide to use custom certificates, you can still use the VMware Certificate Manager utility for certificate replacement. See Replace All Certificates with Custom Certificate (Certificate Manager).

If you encounter problems with vSphere Auto Deploy after replacing certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/2000988.

Request Certificates and Import a Custom Root Certificate

You can use custom certificates from an enterprise or third-party CA. The first step is requesting the certificates from the certificate authority and importing the root certificates into VMware Endpoint Certificate Store (VECS).

The certificate must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
- x509 version 3
- For root certificates, the CA extension must be set to true, and the cert sign must be in the list of requirements.
- SubjectAltName must contain DNS Name=<machine_FQDN>.
- CRT format
- Contains the following Key Usages: Digital Signature, Key Encipherment
- Start time of one day before the current time.
- CN (and SubjectAltName) set to the host name (or IP address) that the ESXi host has in the vCenter Server inventory.

1. Send the Certificate Signing Requests (CSRs) for the following certificates to your enterprise or third-party certificate provider.
   - A machine SSL certificate for each machine. For the machine SSL certificate, the SubjectAltName field must contain the fully qualified domain name (DNS NAME=*machine_FQDN*).
   - Optionally, five solution user certificates for each node. Solution user certificates do not need to include IP address, host name, or email address. Each certificate must have a different certificate Subject.

   Typically, the result is a PEM file for the trusted chain, plus the signed SSL certificates for each vCenter Server node.
2. List the TRUSTED_ROOTS and the machine SSL stores.

   ```
   vecs-cli store list
   ```

   a) Ensure that the current root certificate and all machine SSL certificates are signed by VMCA.
   b) Note down the Serial number, issuer, and Subject CN fields.
   c) Optional: With a Web browser, open an HTTPS connection to a node where the certificate is to be replaced, view the certificate information, and ensure that it matches the machine SSL certificate.
3. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```
4. Publish the custom root certificate.

   ```
   dir-cli trustedcert publish --cert <my_custom_root>
   ```

   If you do not specify a user name and password on the command line, you are prompted.

5. Restart all services.

```
service-control --start --all
```

You can remove the original VMCA root certificate from the certificate store if your company policy requires it. If you do, you have to refresh the vCenter Single Sign-On certificate. See Replace a vCenter Server STS Certificate Using the Command Line.

Replace Machine SSL Certificates with Custom Certificates

After you receive the custom certificates, you can replace each machine certificate.

You must have received a certificate for each machine from your third-party or enterprise CA.

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- CRT format
- x509 version 3
- SubjectAltName must contain DNS Name=<machine_FQDN>.
- Contains the following Key Usages: Digital Signature, Key Encipherment

Perform the steps on each vCenter Server host.

You must have the following information before you can start replacing the certificates:

- Password for administrator@vsphere.local
- Valid Machine SSL custom certificate (`.crt` file)
- Valid Machine SSL custom key (`.key` file)
- Valid custom certificate for Root (`.crt` file)

1. Back up the current machine SSL certificate.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT > oldma-
chine.crt
/usr/lib/vmware-vmafd/bin/vecs-cli entry getkey --store MACHINE_SSL_CERT --alias __MACHINE_CERT > oldma-
chinekey.key
```

2. Log in to each host and add the new machine certificates that you received from the certificate authority to VECS. All hosts need the new certificate in the local certificate store to communicate over SSL.
   a) Delete the existing certificate.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
```

   b) Add the new certificate.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert
 <cert-file-path> --key <key-file-path>
```

3. Extract the hash of the old certificate to be replaced.

```
openssl x509 -in <path_to_old_machinessl_certificate> -noout -sha1 -fingerprint
```

   Output similar to the following appears:

```
SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88
```

4. Update the lookup service registration endpoint manually.

```
/usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/lookupservice/sdk
 --certfile <cert-file-path> --user 'administrator@vsphere.local' --password '<password>' --fingerprint
 <SHA1_hash_of_the_old_certificate_to_replace>
```

5. Restart all services.

```
service-control --stop --all && service-control --start --all
```

Managing Services and Certificates with CLI Commands

You can manage VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store), VMware Directory Service (vmdir), and Security Token Service (STS) certificates by using a set of CLIs. The vSphere Certificate Manager utility supports many related tasks as well, but the CLIs are required for manual certificate management and for managing other services.

You normally access the CLI tools for managing certificates and associated services by using SSH to connect to the appliance shell. See the VMware knowledge base article at http://kb.vmware.com/kb/2100508 for more information.

Manual Certificate Replacement gives examples for replacing certificates using CLI commands.

Table 109: CLI Tools for Managing Certificates and Associated Services

CLI	Description	See
`certool`	Generate and manage certificates and keys. Part of VMCAD, the VMware Certificate Management service.	certool Initialization Commands Reference
`vecs-cli`	Manage the contents of VMware Certificate Store instances. Part of VMware Authentication Framework Daemon (VMAFD).	vecs-cli Command Reference
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	dir-cli Command Reference
`sso-config`	Manage STS certificates.	Command-line help.
`service-control`	Start or stop services, for example as part of a certificate replacement workflow.	Run this command to stop services before running other CLI commands.

CLI Locations

By default, you find the CLIs in the following locations.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

Note: The `service-control` command does not require that you specify the path.

Required Privileges for Running CLIs

Required privileges depend on the CLI that you are using and on the command that you want to run. For example, for most certificate management operations, you have to be an Administrator for the local vCenter Single Sign-On domain (vsphere.local by default). Some commands are available for all users.

dir-cli

You must be a member of the Administrators group in the local domain (vsphere.local by default) to run `dir-cli` commands. If you do not specify a user name and password, you are prompted for the password for the administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.

vecs-cli	Initially, only the store owner and users with blanket access privileges have access to a store. Users in the Administrators group have blanket access privileges. The MACHINE_SSL_CERT and TRUSTED_ROOTS stores are special stores. Only the root user or administrator user, depending on the type of installation, has complete access.
certool	Most of the `certool` commands require that the user is in the Administrators group. All users can run the following commands. • `genselfcacert` • `initscr` • `getdc` • `waitVMDIR` • `waitVMCA` • `genkey` • `viewcert`

Changing the certool Configuration Options

When you run `certool --gencert` or certain other certificate initialization or management commands, the command reads all the values from a configuration file. You can edit the existing file, override the default configuration file with the `--config=<file name>` option, or override values on the command line.

The configuration file, `certool.cfg`, is located in the `/usr/lib/vmware-vmca/share/config/` directory by default.

The file has several fields with the following default values:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Note: As of vSphere 7.0 Update 3o, the OU (organizationalUnitName) field is no longer mandatory.

You can change the values by specifying a modified file on the command line, or by overriding individual values on the command line, as follows.

- Create a copy of the configuration file and edit the file. Use the --config command-line option to specify the file. Specify the full path to avoid path name issues.
- `/usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg`
- Override individual values on the command line. For example, to override Locality, run this command:
  `/usr/lib/vmware-vmca/bin/certool --gencert --privkey=private.key --Locality="Mountain View"`

Specify `--Name` to replace the CN field of the Subject name of the certificate.

- For solution user certificates, the name is <sol_user name>@<domain> by convention, but you can change the name if a different convention is used in your environment.

- For machine SSL certificates, the FQDN of the machine is used.
  VMCA allows only one DNSName (in the `Hostname` field) and no other Alias options. If the IP address is specified by the user, it is stored in SubAltName as well.

Use the `--Hostname` parameter to specify the DNSName of a certificate's SubAltName.

certool Initialization Commands Reference

The `certool` initialization commands allow you to generate certificate signing requests, view and generate certificates and keys that are signed by VMCA, import root certificates, and perform other certificate management operations.

In many cases, you pass a configuration file in to a `certool` command. See Changing the certool Configuration Options. See Replace Existing VMCA-Signed Certificates with New VMCA-Signed Certificates for some usage examples. The command-line help provides details about the options.

certool --initcsr

Generates a Certificate Signing Request (CSR). The command generates a PKCS10 file and a private key.

Option	Description
--gencsr	Required for generating CSRs.
--privkey <key_file>	Name of the private key file.
--pubkey <key_file>	Name of the public key file.
--csrfile <csr_file>	File name for the CSR file to be sent to the CA provider.
--config <config_file>	Name of the configuration file. A sample configuration file is located at `/usr/lib/vmware-vmca/share/config/certool.cfg`. As a best practice, make a copy of the default configuration file and replace the required fields.

Example:

```
certool --gencsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Creates a self-signed certificate and provisions the VMCA server with a self-signed root CA. Using this option is one of the simplest ways to provision the VMCA server. You can instead provision the VMCA server with a third-party root certificate so that VMCA is an intermediate CA. See Use VMCA as an Intermediate Certificate Authority.

This command generates a certificate that is predated by three days to avoid time zone conflicts.

Option	Description
--selfca	Required for generating a self-signed certificate.
--predate <number_of_minutes>	Allows you to set the Valid Not Before field of the root certificate to the specified number of minutes before the current time. This option can be helpful to account for potential time zone issues. The maximum is three days.
--config <config_file>	Name of the configuration file. A sample configuration file is located at `/usr/lib/vmware-vmca/share/config/certool.cfg`. As a best practice, make a copy of the default configuration file and replace the required fields.

Option	Description
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server= 192.0.2.24 --srp-upn=ad-
ministrator@vsphere.local
```

certool --rootca

Imports a root certificate. Adds the specified certificate and private key to VMCA. VMCA always uses the most recent root certificate for signing, but other root certificates remain trusted until you manually delete them. That means you can update your infrastructure one step at a time, and finally delete certificates that you no longer use.

Option	Description
--rootca	Required for importing a root CA.
--cert <certfile>	Name of the certificate file.
--privkey <key_file>	Name of the private key file. This file must be in PEM encoded format.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

Returns the default domain name that is used by vmdir.

Option	Description
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.
--port <port_num>	Optional port number. Defaults to port 389.

Example:

```
certool --getdc
```

certool --waitVMDIR

Wait until the VMware Directory Service is running or until the timeout specified by --wait has elapsed. Use this option along with other options to schedule certain tasks, for example returning the default domain name.

Option	Description
--wait	Optional number of minutes to wait. Defaults to 3.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.
--port <port_num>	Optional port number. Defaults to port 389.

Example:

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

Wait until the VMCA service is running or until the specified timeout has elapsed. Use this option in conjunction with other options to schedule certain tasks, for example, generating a certificate.

Option	Description
--wait	Optional number of minutes to wait. Defaults to 3.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.
--port <port_num>	Optional port number. Defaults to port 389.

Example:

```
certool --waitVMCA --selfca
```

certool --publish-roots

Forces an update of root certificates. This command requires administrative privileges.

Option	Description
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --publish-roots
```

certool Management Commands Reference

The `certool` management commands allow you to view, generate, and revoke certificates and to view information about certificates.

certool --genkey

Generates a private and public key pair. Those files can then be used to generate a certificate that is signed by VMCA.

Option	Description
--genkey	Required for generating a private and public key.
--privkey <keyfile>	Name of the private key file.
--pubkey <keyfile>	Name of the public key file.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

Generates a certificate from the VMCA server. This command uses the information in `certool.cfg` or in the specified configuration file. You can use the certificate to provision machine certificates or solution user certificates.

Option	Description
--gencert	Required for generating a certificate.
--cert <certfile>	Name of the certificate file. This file must be in PEM encoded format.
--privkey <keyfile>	Name of the private key file. This file must be in PEM encoded format.
--config <config_file>	Name of the configuration file. A sample configuration file is located at `/usr/lib/vmware-vmca/share/config/certool.cfg`. As a best practice, make a copy of the default configuration file and replace the required fields.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --gencert --privkey=<filename> --cert=<filename> --config=<config_file>
```

certool --getrootca

Prints the current root CA certificate in human-readable form. This output is not usable as a certificate, it is changed to be human readable.

Option	Description
--getrootca	Required for printing the root certificate.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --getrootca --server=remoteserver
```

certool --viewcert

Print all the fields in a certificate in human-readable form.

Option	Description
--viewcert	Required for viewing a certificate.
--cert <certfile>	Name of the configuration file. A sample configuration file is located at `/usr/lib/vmware-vmca/share/config/certool.cfg`. As a best practice, make a copy of the default configuration file and replace the required fields.

Example:

```
certool --viewcert --cert=<filename>
```

certool --enumcert

List all certificates that the VMCA server knows about. The required filter option lets you list all certificates or only revoked, active, or expired certificates.

Option	Description
--enumcert	Required for listing all certificates.
--filter [all | active]	Required filter. Specify all or active. The revoked and expired options are not currently supported.

Example:

```
certool --enumcert --filter=active
```

certool --status

Sends a specified certificate to the VMCA server to check whether the certificate has been revoked. Prints `Certificate: REVOKED` if the certificate is revoked, and `Certificate: ACTIVE` otherwise.

Option	Description
--status	Required to check the status of a certificate.
--cert <certfile>	Name of the configuration file. A sample configuration file is located at `/usr/lib/vmware-vmca/share/config/certool.cfg`. As a best practice, make a copy of the default configuration file and replace the required fields.
--server <server>	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --status --cert=<filename>
```

certool --genselfcacert

Generates a self-signed certificate based on the values in the configuration file. This command generates a certificate that is predated by three days to avoid time zone conflicts.

Option	Description
--genselfcacert	Required for generating a self-signed certificate.
--outcert <cert_file>	Name of the certificate file. This file must be in PEM encoded format.
--outprivkey <key_file>	Name of the private key file. This file must be in PEM encoded format.
--config <config_file>	Name of the configuration file. A sample configuration file is located at `/usr/lib/vmware-vmca/share/config/certool.cfg`. As a best practice, make a copy of the default configuration file and replace the required fields.

Example:

```
certool --genselfcert --privkey=<filename> --cert=<filename> --config=<config_file>
```

vecs-cli Command Reference

The `vecs-cli` command set allows you to manage instances of VMware Certificate Store (VECS). Use these commands together with `dir-cli` and `certool` to manage your certificate infrastructure and authentication services.

vecs-cli store create

Creates a certificate store.

Option	Description
--name <name>	Name of the certificate store.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

Example:

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Deletes a certificate store. You cannot delete the MACHINE_SSL_CERT, TRUSTED_ROOTS and TRUSTED_ROOT_CRLS system stores. Users with required privileges can delete solution user stores.

Option	Description
--name <name>	Name of the certificate store to delete.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

Example:

```
vecs-cli store delete --name <store>
```

vecs-cli store list

List certificate stores.

Option	Description
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.

Option	Description
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

VECS includes the following stores.

Table 110: Stores in VECS

Store	Description
Machine SSL store (MACHINE_SSL_CERT)	• Used by the reverse proxy service on every vSphere node. • Used by the VMware Directory Service (vmdir) on each vCenter Server node. All services in vSphere 6.0 and later communicate through a reverse proxy, which uses the machine SSL certificate. For backward compatibility, the 5.x services still use specific ports. As a result, some services such as vpxd still have their own port open.
Solution user stores • `machine` • `vpxd` • `vpxd-extension` • `vsphere-webclient` • `wcp`	VECS includes one store for each solution user. The subject of each solution user certificate must be unique, for example, the machine certificate cannot have the same subject as the vpxd certificate. Solution user certificates are used for authentication with vCenter Single Sign-On. vCenter Single Sign-On checks that the certificate is valid, but does not check other certificate attributes. The following solution user certificate stores are included in VECS: • `machine` : Used by the license server and the logging service. **Note:** The machine solution user certificate has nothing to do with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine. • `vpxd` : vCenter service daemon (vpxd) store. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On. • `vpxd-extension` : vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users. • `vsphere-webclient` : vSphere Client store. Also includes some additional services such as the performance chart service. • `wcp` : VMware vSphere® with VMware Tanzu™ store. Also used for vSphere Cluster Services. Each vCenter Server node includes a `machine` certificate.
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.
vSphere Certificate Manager Utility backup store (BACKUP_STORE)	Used by VMCA (VMware Certificate Manager) to support certificate revert. Only the most recent state is stored as a backup, you cannot go back more than one step.

Store	Description
Other stores	Other stores might be added by solutions. For example, the Virtual Volumes solution adds an SMS store. Do not modify the certificates in those stores unless VMware documentation or a VMware Knowledge Base article instructs you to do so. **Note:** Deleting the TRUSTED_ROOTS_CRLS store can damage your certificate infrastructure. Do not delete or modify the TRUSTED_ROOTS_CRLS store.

Example:

```
vecs-cli store list
```

vecs-cli store permissions

Grants or revokes permissions to the store. Use either the --grant or the --revoke option.

The owner of the store can perform all operations, including granting and revoking permissions. The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default, has all privileges on all stores, including granting and revoking permissions.

You can use `vecs-cli get-permissions --name <store-name>` to retrieve the current settings for the store.

Option	Description
--name <name>	Name of the certificate store.
--user <username>	Unique name of the user who is granted permissions.
--grant [read|write]	Permission to grant, either read or write.
--revoke [read|write]	Permission to revoke, either read or write. Not currently supported.

vecs-cli store get-permissions

Retrieves the current permission settings for the store.

Option	Description
--name <name>	Name of the certificate store.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry create

Creates an entry in VECS. Use this command to add a private key or certificate to a store.

Note: Do not use this command to add root certificates to the TRUSTED_ROOTS store. Instead, use the `dir-cli` command to publish root certificates.

Option	Description
--store <NameOfStore>	Name of the certificate store.
--alias <Alias>	Optional alias for the certificate. This option is ignored for the trusted root store.
--cert <certificate_file_path>	Full path of the certificate file.
--key <key-file-path>	Full path of the key that corresponds to the certificate. Optional.
--password <password>	Optional password for encrypting the private key.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry list

Lists all entries in a specified store.

Option	Description
--store <NameOfStore>	Name of the certificate store.

vecs-cli entry getcert

Retrieves a certificate from VECS. You can send the certificate to an output file or display it as human-readable text.

Option	Description
--store <NameOfStore>	Name of the certificate store.
--alias <Alias>	Alias of the certificate.
--output <output_file_path>	File to write the certificate to.
--text	Displays a human-readable version of the certificate.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry getkey

Retrieves a key that is stored in VECS. You can send the key to an output file or display it as human-readable text.

Option	Description
--store <NameOfStore>	Name of the certificate store.
--alias <Alias>	Alias for the key.

Option	Description
--output <output_file_path>	Output file to write the key to.
--text	Displays a human-readable version of the key.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry delete

Deletes an entry in a certificate store. If you delete an entry in VECS, you permanently remove it from VECS. The only exception is the current root certificate. VECS polls vmdir for a root certificate.

Option	Description
--store <NameOfStore>	Name of the certificate store.
--alias <Alias>	Alias for the entry you want to delete.
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.
-y	Suppresses the confirmation prompt. For advanced users only.

vecs-cli force-refresh

Forces a refresh of VECS. By default, VECS polls vmdir for new root certificate files every 5 minutes. Use this command for an immediate update of VECS from vmdir.

Option	Description
--server <server-name>	Used to specify a server name if you connect to a remote VECS instance.
--upn <user-name>	User Principle Name that is used to log in to the server instance specified by --server <server-name> . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

dir-cli Command Reference

The `dir-cli` utility supports creation and updates to solution users, account management, and management of certificates and passwords in VMware Directory Service (vmdir). You can use `dir-cli` to manage and query the domain functional level of vCenter Server instances.

dir-cli nodes list

Lists all the enhanced linked mode connected vCenter Server systems.

Option	Description
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.
--server <psc_ip_or_fqdn>	Use this option to connect to another vCenter Server to see its replication partners.

dir-cli computer password-reset

Enables you to reset the password of the machine account in the domain.

Option	Description
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.
--live-dc-hostname <server name>	Current name of the vCenter Server instance.

dir-cli service create

Creates a solution user. Primarily used by third-party solutions.

Option	Description
--name <name>	Name of the solution user to create
--cert <cert file>	Path to the certificate file. This can be a certificate signed by VMCA or a third-party certificate.
--ssogroups <comma-separated-groupnames>	Makes the solution user a member of the specified groups.
--wstrustrole <ActAsUser>	Makes the solution user a member of the built-in administrators or users group. In other words, determines whether the solution user has administrative privileges.
--ssoadminrole <Administrator/User>	Makes the solution user a member of the ActAsUser group. The ActAsUser role enables users to act on behalf of other users.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli service list

List the solution users that `dir-cli` knows about.

Option	Description
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.

Option	Description
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli service delete

Delete a solution user in vmdir. When you delete the solution user, all associated services become unavailable to all management nodes that use this instance of vmdir.

Option	Description
--name	Name of the solution user to delete.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli service update

Updates the certificate for a specified solution user, that is, collection of services. After running this command, update the solution user certificate entry in VECS by running the `vecs-cli entry create` command. See vecs-cli Command Reference.

Option	Description
--name <name>	Name of the solution user to update.
--cert <cert_file>	Name of the certificate to assign to the service.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user create

Creates a regular user inside vmdir. This command can be used for human users who authenticate to vCenter Single Sign-On with a user name and password. Use this command only during prototyping.

Option	Description
--account <name>	Name of the vCenter Single Sign-On user to create.
--user-password <password>	Initial password for the user.
--first-name <name>	First name for the user.
--last-name <name>	Last name for the user.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user modify

Modifies the specified user inside vmdir.

Option	Description
--account <name>	Name of the vCenter Single Sign-On user to modify.
--password-never-expires	Set this option to true if you are modifying a user account for automated tasks that have to authenticate to vCenter Server, and you want to ensure that the tasks do not stop running because of password expiration. Use this option with care.
--password-expires	Set this option to true if you want to revert the --password-never-expires option.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user delete

Deletes the specified user inside vmdir.

Option	Description
--account <name>	Name of the vCenter Single Sign-On user to delete.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user find-by-name

Finds a user inside vmdir by name. The information that this command returns depends on what you specify in the `--level` option.

Option	Description
--account <name>	Name of the vCenter Single Sign-On user to find.
--level <info level 0|1|2>	Returns the following information: • Level 0 - Account and UPN • Level 1 - level 0 info + First and last name • Level 2 : level 0 + Account disabled flag, Account locked flag, Password never expires flag, password expired flag and password expiry flag. The default level is 0.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli group modify

Adds a user or group to an existing group.

Option	Description
--name <name>	Name of the group in vmdir.
--add <user_or_group_name>	Name of the user or group to add.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli group list

Lists a specified vmdir group.

Option	Description
--name <name>	Optional name of the group in vmdir. This option allows you to check whether a specific group exists.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli ssogroup create

Create a group inside the local domain (vsphere.local by default).

Use this command if you want to create groups to manage user permissions for the vCenter Single Sign-On domain. For example, if you create a group and then add it to the Administrators group of the vCenter Single Sign-On domain, then all users that you add to that group have administrator permissions for the domain.

It is also possible to give permissions to vCenter inventory objects to groups in the vCenter Single Sign-On domain. See the *vSphere Security* documentation.

Option	Description
--name <name>	Name of the group in vmdir. Maximum length is 487 characters.
--description <description>	Optional description for the group.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli trustedcert publish

Publishes a trusted root certificate to vmdir. After running this command, VECS picks up the certificate change after one minute, or you can run the `vecs-cli force-refresh` command to sync the certificate immediately.

Option	Description
--cert <file>	Path to certificate file.
--crl <file>	This option is not supported by VMCA.

Option	Description
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.
--chain	Specify this option if you are publishing a chained certificate. No option value is needed.

dir-cli trustedcert unpublish

Unpublishes a trusted root certificate currently in vmdir. Use this command, for example, if you added a different root certificate to vmdir that is now the root certificate for all other certificates in your environment. Unpublishing certificates that are no longer in use is part of hardening your environment.

Option	Description
--cert-file <file>	Path to the certificate file to unpublish
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli trustedcert list

Lists all trusted root certificates and their corresponding IDs. You need the certificate IDs to retrieve a certificate with `dir-cli trustedcert get`.

Option	Description
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli trustedcert get

Retrieves a trusted root certificate from vmdir and writes it to a specified file.

Option	Description
--id <cert_ID>	ID of the certificate to retrieve. The `dir-cli trustedcert list` command shows the ID.
--outcert <path>	Path to write the certificate file to.
--outcrl <path>	Path to write the CRL file to. Not currently used.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli password create

Creates a random password that meets the password requirements. This command can be used by third-party solution users.

Option	Description
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli password reset

Allows an administrator to reset a user's password. If you are a non-administrator user who wants to reset a password, use `dir-cli password change` instead.

Option	Description
--account	Name of the account to assign a new password to.
--new	New password for the specified user.
--login <admin_user_id>	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
--password <admin_password>	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli password change

Allows a user to change their password. You must be the user who owns the account to make this change. Administrators can use `dir-cli password reset` to reset any password.

Option	Description
--account	Account name.
--current	Current password of the user who owns the account.
--new	New password of the user who owns the account.

vSphere Authentication with vCenter Single Sign-On

vCenter Single Sign-On is an authentication broker and security token exchange infrastructure. vCenter Single Sign-On issues a token when a user authenticates. The user can use the token to authenticate to vCenter Server services. The user can then perform the actions that user has privileges for.

Because traffic is encrypted for all communications, and because only authenticated users can perform the actions that they have privileges for, your environment is secure.

Users and service accounts authenticate with a token, or a user name and password. Solution users authenticate with a certificate.

The next step is authorizing the users who can authenticate to perform certain tasks. Usually, you assign vCenter Server privileges, typically by assigning the user to a group that has a role. vSphere includes other permission models such as global permissions. See the *vSphere Security* documentation.

How vCenter Single Sign-On Protects Your Environment

vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism.

vCenter Single Sign-On uses the following services.

- Authentication of users through either external identity provider federation or the vCenter Server built-in identity provider. The built-in identity provider supports local accounts, Active Directory or OpenLDAP, Integrated Windows Authentication (IWA), and miscellaneous authentication mechanisms (smart card, RSA SecurID, and Windows Session Authentication).
- Authentication of solution users through certificates.
- Security Token Service (STS).
- SSL for secure traffic.

Identity Provider Overview

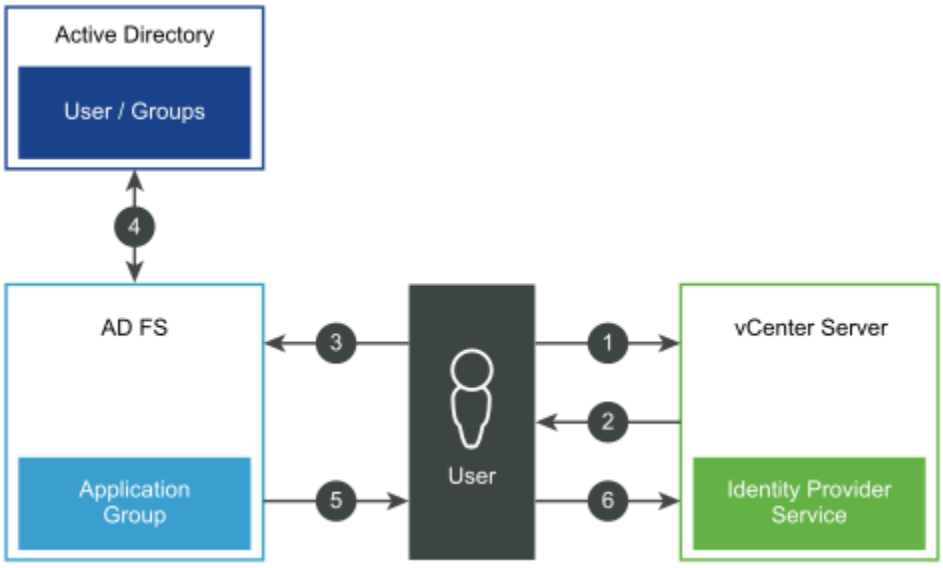
Before vSphere 7.0, vCenter Server includes a built-in identity provider. By default, vCenter Server uses the vsphere.local domain as the identity source (but you can change it during installation). You can configure the vCenter Server built-in identity provider to use Active Directory (AD) as its identity source using LDAP/S, OpenLDAP/S, and Integrated Windows Authentication (IWA). Such configurations allow customers to log in to vCenter Server using their AD accounts.

Starting with vSphere 7.0, you can configure vCenter Server for an external identity provider using federated authentication. In such a configuration, you replace vCenter Server as the identity provider. Currently, vSphere supports Active Directory Federation Services (AD FS) as the external identity provider. In this configuration, AD FS interacts with the identity sources on behalf of vCenter Server.

User Login with vCenter Server Identity Provider Federated Authentication

The following figure shows the user login flow for vCenter Server Identity Provider Federation.

Figure 44: vCenter Server Identity Provider Federation User Login



vCenter Server, AD FS, and Active Directory interact as follows:

1. The user starts on the vCenter Server landing page by entering a user name.
2. If the user name is for a federated domain, vCenter Server redirects the authentication request to AD FS.
3. If needed, AD FS prompts the user to log in with Active Directory credentials.

4. AD FS authenticates the user with Active Directory.
5. AD FS issues a security token with group information from Active Directory.
6. vCenter Server uses the token to log in the user.

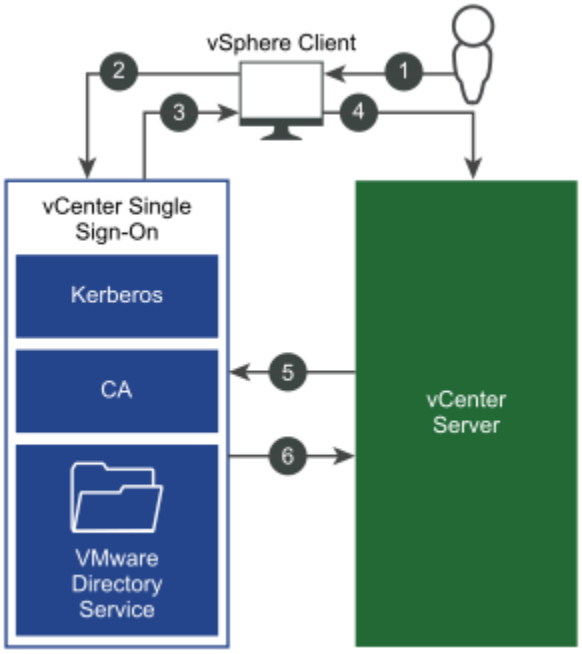
The user is now authenticated, and can view and modify any objects that the user's role has privileges for.

In case the external identity provider is unreachable, the login process falls back to the vCenter Server landing page, showing an appropriate information message. Users can still log in using their local accounts in the vsphere.local identity source.

User Login with the vCenter Server Built-In Identity Provider

The following figure shows the user login flow when vCenter Server acts as the identity provider.

Figure 45: User Login with the vCenter Server Built-In Identity Provider



1. A user logs in to the vSphere Client with a user name and password to access the vCenter Server system or another vCenter service.
   When Integrated Windows Authentication (IWA) has been configured, users can also log in without having to reenter their Windows password by checking the **Use Windows session authentication** check box.
2. The vSphere Client passes the login information to the vCenter Single Sign-On service, which checks the SAML token of the vSphere Client. If the vSphere Client has a valid token, vCenter Single Sign-On then checks whether the user is in the configured identity source (for example Active Directory).
   - If only the user name is used, vCenter Single Sign-On checks in the default domain.
   - If a domain name is included with the user name (*DOMAIN*\user1 or user1@*DOMAIN*), vCenter Single Sign-On checks that domain.
3. If the user can authenticate to the identity source, vCenter Single Sign-On returns a token that represents the user to the vSphere Client.
4. The vSphere Client passes the token to the vCenter Server system.
5. vCenter Server checks with the vCenter Single Sign-On server that the token is valid and not expired.
6. The vCenter Single Sign-On server returns the token to the vCenter Server system, using the vCenter Server Authorization Framework to allow user access.

The user is now authenticated, and can view and modify any objects that the user's role has privileges for.

Supported Encryption

AES encryption, which is the highest level of encryption, is supported. The supported encryption affects security when vCenter Single Sign-On uses Active Directory as an identity source.

Understanding vCenter Server Identity Provider Federation

Starting in vSphere 7.0, vCenter Server supports federated authentication to sign in to vCenter Server.

To enable federated authentication to vCenter Server, you configure a connection to an external identity provider. The identity provider instance that you configure replaces vCenter Server as the identity provider. Currently, vCenter Server supports only Active Directory Federation Services (AD FS) as an external identity provider.

Note: VMware encourages you to use federated authentication as vSphere moves towards token-based authentication. vCenter Server continues to have local accounts, for administrative access and error recovery.

How vCenter Server Identity Provider Federation Works

vCenter Server Identity Provider Federation enables you to configure an external identity provider for federated authentication. In this configuration, the external identity provider interacts with the identity source on behalf of vCenter Server.

vCenter Server Identity Provider Federation Basics

Starting in vSphere 7.0, vCenter Server supports federated authentication. In this scenario, when a user logs in to vCenter Server, vCenter Server redirects the user login to the external identity provider. The user credentials are no longer provided to vCenter Server directly. Instead, the user provides credentials to the external identity provider. vCenter Server trusts the external identity provider to perform the authentication. In the federation model, users never provide credentials directly to any service or application but only to the identity provider. As a result, you "federate" your applications and services, such as vCenter Server, with your identity provider.

vCenter Server Identity Provider Federation Benefits

vCenter Server Identity Provider Federation provides the following benefits.

- You can use Single Sign-On with existing federated infrastructure and applications.
- You can improve data center security because vCenter Server never handles the user’s credentials.
- You can use the authentication mechanisms, such as multi-factor authentication, supported by the external identity provider.

vCenter Server Identity Provider Federation Components

The following components comprise a vCenter Server Identity Provider Federation configuration that uses Microsoft Active Directory Federation Services (AD FS):

- A vCenter Server
- An identity provider service configured on the vCenter Server
- An AD FS server and associated Microsoft Active Directory domain
- An AD FS Application Group
- Active Directory groups and users that map to vCenter Server groups and users

Note: Currently, vCenter Server supports only AD FS as an external identity provider.

vCenter Server Identity Provider Federation Architecture

In vCenter Server Identity Provider Federation, vCenter Server uses the OpenID Connect (OIDC) protocol to receive an identity token that authenticates the user with vCenter Server.

To establish a relying party trust between vCenter Server and an identity provider, you must establish the identifying information and a shared secret between them. In AD FS, you do so by creating an OIDC configuration known as an Application Group, which consists of a Server application and a Web API. The two components specify the information that vCenter Server uses to trust and communicate with the AD FS server. You also create a corresponding identity provider in vCenter Server. Finally, you configure group memberships in vCenter Server to authorize logins from users in the AD FS domain.

The AD FS administrator must provide the following information to create the vCenter Server identity provider configuration:

- Client Identifier: The UUID string that is generated by the AD FS Application Group wizard and that identifies the Application Group itself.
- Shared Secret: The secret that is generated by the AD FS Application Group wizard and that is used to authenticate vCenter Server with AD FS.
- OpenID Address: The OpenID Provider Discovery endpoint URL of the AD FS server, specifying a well-known address that is typically the issuer endpoint concatenated with the path "`/.well-known/openid-configuration`". For example: `https://webserver.example.com/adfs/.well-known/openid-configuration`.

vCenter Server Identity Provider Federation and Enhanced Linked Mode

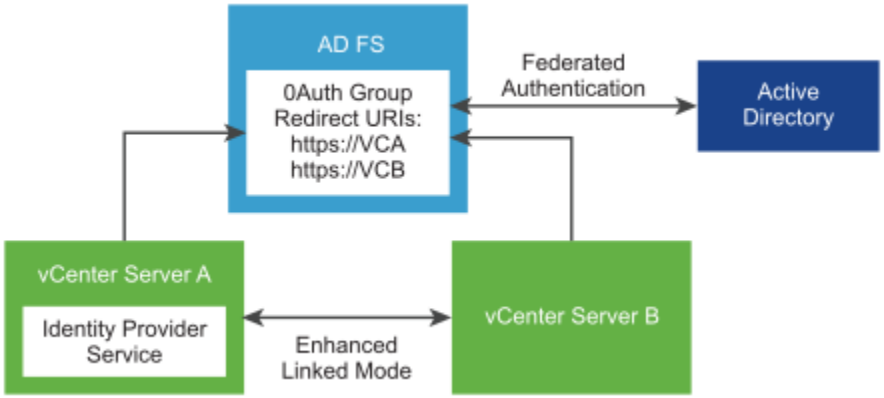
When you enable Identity Provider Federation in vCenter Server environments using enhanced linked mode, authentication and workflows continue to work as before.

If you use Enhanced Linked Mode configuration, note the following when logging in to vCenter Server using federated authentication.

- Users continue to see the same inventory, and can perform the same actions, based on the vCenter Server permissions and roles model.
- vCenter Server hosts in enhanced linked mode are not required to have access to each other's identity providers. For example, consider two vCenter Server systems A and B, and that use enhanced linked mode. After vCenter Server A authorizes a user, then the user is authorized on vCenter Server B as well.

The following illustration shows the authentication workflow with enhanced linked mode and vCenter Server Identity Provider Federation.

Figure 46: Enhanced Linked Mode and vCenter Server Identity Provider Federation



1. Two vCenter Server nodes are deployed in Enhanced Linked Mode configuration.

2. The AD FS setup has been configured on vCenter Server A using the Change Identity Provider wizard in the vSphere Client. Group memberships and permissions have also been established for AD FS users or groups.
3. vCenter Server A replicates the AD FS configuration to vCenter Server B.
4. All Redirect URIs for both vCenter Server nodes are added to the OAuth Application Group in AD FS. Only one OAuth Application Group is created.
5. When a user logs into and is authorized by vCenter Server A, the user is also authorized on vCenter Server B. If the user logs in to vCenter Server B first, the same holds true.

vCenter Server enhanced linked mode supports the following configuration scenarios for identity provider federation. In this section, the terms "AD FS settings" and "AD FS configuration" refer to the settings that you configure in the vSphere Client using the Change Identity Provider wizard, and any group memberships or permissions that you have established for AD FS users or groups.

Enable AD FS on an existing Enhanced Linked Mode configuration	High-level steps: 1. Deploy N vCenter Server nodes in Enhanced Linked Mode configuration. 2. Configure AD FS on one of the linked vCenter Server nodes. 3. The AD FS configuration is replicated to all other (N-1) vCenter Server nodes. 4. Add all Redirect URIs for all N vCenter Server nodes to the configured OAuth Application Group in AD FS.
Link a new vCenter Server to an existing Enhanced Linked Mode AD FS configuration	High-level Steps: 1. (Prerequisite) Set up AD FS on a vCenter Server N-node Enhanced Linked Mode configuration. 2. Deploy a new independent vCenter Server node. 3. Repoint the new vCenter Server to the N-node AD FS enhanced linked mode domain, using one of the N nodes as its replication partner. 4. All AD FS settings in the existing Enhanced Linked Mode configuration are replicated to the new vCenter Server. The AD FS settings that are in the N-node AD FS enhanced linked mode domain overwrite any existing AD FS settings on the newly linked vCenter Server. 5. Add all Redirect URIs for the new vCenter Server to the existing configured OAuth Application Group in AD FS.
Unlink a vCenter Server from an Enhanced Linked Mode AD FS configuration	High-level steps: 1. (Prerequisite) Set up AD FS on an N-node vCenter Server Enhanced Linked Mode configuration. 2. Unregister one of the vCenter Server hosts in the N-node configuration and repoint it to a new domain to unlink it from the N-node configuration. 3. The domain repointing process does not preserve SSO settings, so all AD FS settings on the unlinked vCenter Server node are reverted and lost. To continue using AD FS on this vCenter Server unlinked node, you must reconfigure AD FS from the beginning or you must relink the vCenter Server to an Enhanced Linked Mode configuration where AD FS is already set up.

vCenter Server Identity Provider Federation Caveats and Interoperability

vCenter Server Identity Provider Federation can interoperate with many other VMware features.

As you are planning your vCenter Server Identity Provider Federation strategy, consider possible interoperability limitations.

Authentication Mechanisms

In a vCenter Server Identity Provider Federation configuration, the external identity provider handles the authentication mechanisms (passwords, MFA, biometrics, and so on).

Support for a Single Active Directory Domain

When you configure vCenter Server Identity Provider Federation, the Configure Main Identity Provider wizard prompts you to enter LDAP information for the AD domain that contains the users and groups you want to access vCenter Server. vCenter Server derives the AD domain to use for authorization and permissions from the User Base DN that you specify in the wizard. You can add permissions on vSphere objects only for users and groups from this AD domain. Users or groups from AD child domains or other domains in the AD forest are not supported by vCenter Server Identity Provider Federation.

vCenter Server Policies

When vCenter Server acts as the identity provider, you control vCenter Server password, lockout, and token policies for the vsphere.local domain. When using federated authentication with vCenter Server, the external identity provider controls the password, lockout, and token policies for the accounts stored in the identity source such as Active Directory.

Auditing and Compliance

When using vCenter Server Identity Provider Federation, vCenter Server continues to create log entries for successful user logins. However, the external identity provider is responsible for tracking and logging actions such as failed password-entry attempts and user account lockouts. vCenter Server does not log such events because they are no longer visible to vCenter Server. For example, when AD FS is the identity provider, AD FS tracks and logs errors for federated logins. When vCenter Server is the identify provider for local logins, vCenter Server tracks and logs errors for local logins. In a federated configuration, vCenter Server does continue to log user actions post-login.

Existing VMware Product Integration

VMware products integrated with vCenter Server (for example, vROps, vSAN, NSX, and so on) continue to work as before.

Products That Integrate Post-Login

Products that integrate post-login (that is, they do not require a separate login) continue to work as before.

Simple Authentication for API, SDK, and CLI Access

Existing scripts, products, and other functionality that rely on API, SDK, or CLI commands that use Simple Authentication (that is, user name and password) continue to work as before. Internally, authentication occurs by passing the user name and password. This passing of the user name and password compromises some of the benefits of using identity federation, because it exposes the password to vCenter Server (and your scripts). Consider migrating to token-based authentication where possible.

vCenter Server Management Interface

If the user is a member of the Administrators group, accessing the vCenter Server Management Interface (formerly called vCenter Server Appliance Management Interface or VAMI) is supported.

Entering User Name Text on the AD FS Login Page

The AD FS login page does not support passing text to pre-populate the user name text box. As a result, during federated logins with AD FS, after entering your user name on the vCenter Server landing page and redirecting to the AD FS login page, you must reenter your user name on the AD FS login page. The user name that you enter on the vCenter Server landing page is necessary to redirect the login to the appropriate identity provider, and the user name on the AD FS login page is necessary to authenticate with AD FS. This inability to pass the user name to the AD FS login page is a limitation of AD FS. You cannot configure or change this behavior directly from vCenter Server.

vCenter Server Identity Provider Federation Life Cycle

When managing the life cycle of vCenter Server Identity Provider Federation, there are some specific considerations.

You can manage your vCenter Server Identity Provider Federation life cycle in the following ways.

Migrating from Using Active Directory to AD FS

If you are using Active Directory as your identity source for vCenter Server, migrating to using AD FS is straight forward. If your Active Directory groups and roles match your AD FS groups and roles, you do not need to take any additional action. When the groups and roles do not match, then you must perform some additional work. If vCenter Server is a domain member, consider removing it from the domain as it is not needed or used for identity federation.

Cross-Domain Repointing and Migration

vCenter Server Identity Provider Federation supports cross-domain repointing, that is, moving a vCenter Server from one vSphere SSO domain to another. The repointed vCenter Server receives the replicated AD FS configuration from the vCenter Server system, or systems, to which it was pointed.

In general, you do not need to perform any additional AD FS reconfiguration for a cross-domain repoint, unless one of the following is true.

1. The AD FS configuration of the repointed vCenter Server differs from the AD FS configuration of the vCenter Server to which it was pointed.
2. This is the first time the repointed vCenter Server is receiving an AD FS configuration.

In these cases, you must add the vCenter Server system's Redirect URIs to the corresponding Application Group on the AD FS server. For example, if vCenter Server 1 with AD FS Application Group A (or no AD FS configuration) is repointed to vCenter Server 2 with AD FS Application Group B, you must add the Redirect URIs of vCenter Server 1 to Application Group B.

Configuring vCenter Server Identity Provider Federation

After you deploy vCenter Server initially, you can configure an external identity provider for federated authentication.

You configure vCenter Server Identity Provider Federation from the vSphere Client or the API. You also must perform some configuration on your external identity provider. To configure vCenter Server Identity Provider Federation, you must have vCenter Single Sign-On administrator privileges. Having vCenter Single Sign-On administrator privileges is different from having the Administrator role on vCenter Server or ESXi. In a new installation, only the vCenter Single Sign-On administrator (administrator@vsphere.local by default) can authenticate to vCenter Single Sign-On.

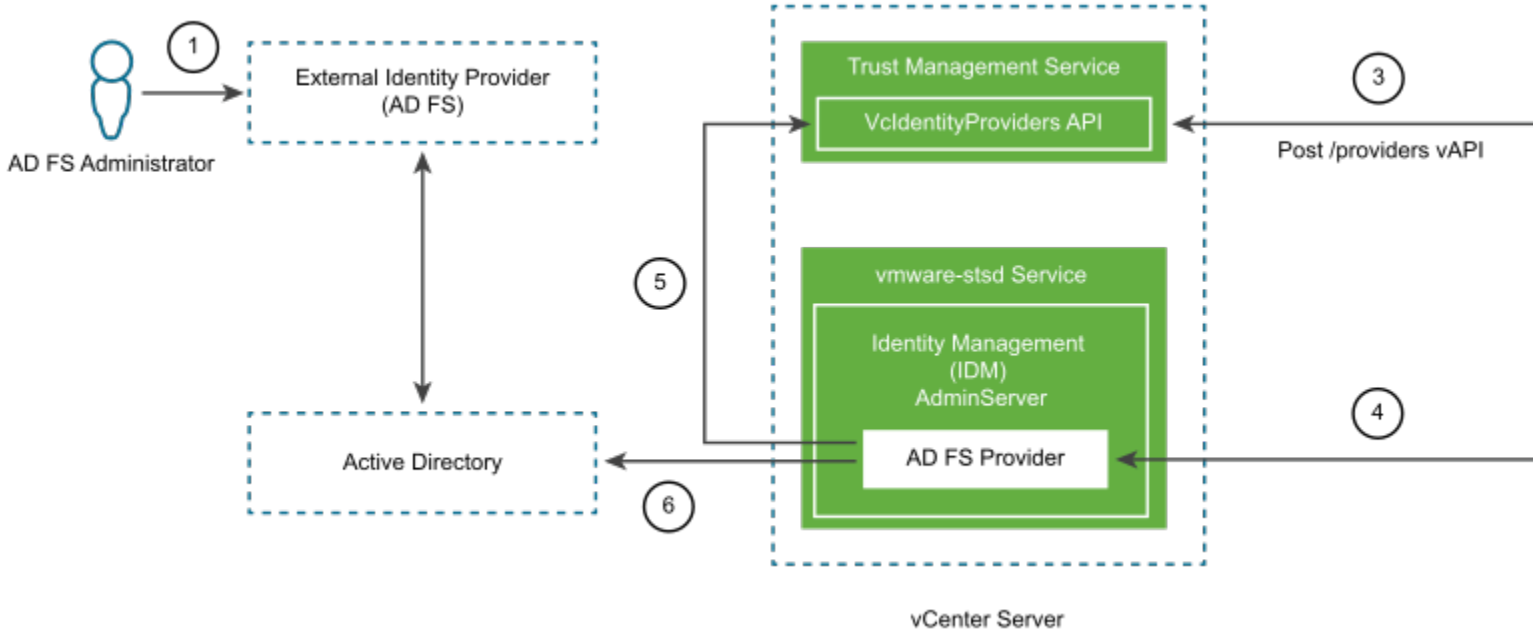
vCenter Server Identity Provider Federation Configuration Process Flow

To configure vCenter Server Identity Provider Federation effectively, you must understand the communication flows that take place.

vCenter Server Identity Provider Federation Configuration Process Flow

The following figure shows the process flow that occurs when configuring vCenter Server Identity Provider Federation.

Figure 47: vCenter Server Identity Provider Federation Configuration Process Flow



vCenter Server, AD FS, and Active Directory interact as follows.

1. The AD FS administrator configures an AD FS OAuth Application for vCenter Server.
2. The vCenter Server administrator logs in to the vCenter Server using the vSphere Client.
3. The vCenter Server administrator adds an AD FS identity provider to vCenter Server, and also enters information about the Active Directory domain.
   vCenter Server needs this information to make an LDAP connection to the Active Directory domain of the AD FS server. Using this connection, vCenter Server searches for users and groups, and adds them to vCenter Server local groups in the next step. See the section titled "Searching the Active Directory Domain" that follows for more information.
4. The vCenter Server administrator configures authorization permissions in vCenter Server for AD FS users.
5. The AD FS Provider queries the VcIdentityProviders API to get the LDAP connection information for the Active Directory source.
6. The AD FS Provider searches Active Directory for the queried users or groups to finish the Authorization configuration.

Searching the Active Directory Domain

You configure AD FS as the external identity provider in vCenter Server by using the Configure Main Identity Provider wizard in the vSphere Client. As part of the configuration process, you must enter information about your Active Directory domain, including user and group distinguished name information. Configuration of AD FS for authentication requires this Active Directory connection information. This connection is necessary to search for and map Active Directory user names and groups to roles and permissions in vCenter Server, whereas AD FS is used for the authentication of the user. This step of the Configure Main Identity Provider wizard does not create an Active Directory Over LDAP identity source. Rather, vCenter Server uses this information to establish a valid search-capable connection to your Active Directory domain to find users and groups there.

Consider an example using the following distinguished name entries:

- Base distinguished name for users: cn=Users,dc=corp,dc=local
- Base distinguished name for groups: dc=corp,dc=local
- User name: cn=Administrator,cn=Users,dc=corp,dc=local

If the AdfsUser@corp.local user is a member of the ADGroup@corp.local group, entering this information in the wizard allows a vCenter Server administrator to search for and find the ADGroup@corp.local group and add it to the vCenter Server Administrators@vsphere.local group. As a result, the AdfsUser@corp.local user is granted administrative privileges in vCenter Server upon logging in.

vCenter Server also uses this search process when you configure global permissions for Active Directory users and groups. In both cases, either configuring global permissions, or adding a user or group, you select the domain you entered for your AD FS identify provider from the **Domain** drop-down menu to search for and select users and groups from your Active Directory domain.

Use the Trusted Root Certificates Store Instead of the JRE truststore

If you imported a root CA certificate issued by your own internal Certificate Authority to the JRE truststore in vSphere 7.0, starting in vSphere 7.0 Update 1, you can register the certificate to the Trusted Root Certificates Store.

To configure vCenter Server Identity Provider Federation in vSphere 7.0 with a root CA certificate that was issued by your own internal Certificate Authority, you had to import it to the JRE truststore. Starting in vSphere 7.0 Update 1, you can register the certificate to the Trusted Root Certificates Store. This change means that you should add the root CA certificate that was issued by your own internal Certificate Authority to the Trusted Root Certificates Store (also called the VMware Endpoint Certificate Store, or VECS). Certificates in the JRE truststore continue to function, however, vCenter Server is standardizing on using the Trusted Root Certificates Store.

1. Log in with the vSphere Client to the vCenter Server.
2. Navigate to **Administration** > **Certificates** > **Certificate Management**.
3. Next to **Trusted Root Certificates**, click **Add**.
4. Browse for the AD FS root certificate and click **Add**.
   The certificate is added in a panel under **Trusted Root Certificates**.

Configure vCenter Server Identity Provider Federation for AD FS

After installing or upgrading to vSphere 7.0 or later, you can configure vCenter Server Identity Provider Federation.

Active Directory Federation Services requirements:

- AD FS for Windows Server 2016 or later must already be deployed.
- AD FS must be connected to Active Directory.
- An Application Group for vCenter Server must be created in AD FS as part of the configuration process. See the VMware knowledge base article at https://kb.vmware.com/s/article/78029.
- An AD FS server certificate (or a CA or intermediate certificate that signed the AD FS server certificate) that you add to the Trusted Root Certificates Store.
- You have created a vCenter Server administrators group in AD FS that contains the users you want to grant vCenter Server administrator privileges to.

For more information about configuring AD FS, see the Microsoft documentation.

vCenter Server and other requirements:

- vSphere 7.0 or later

- vCenter Server must be able to connect to the AD FS discovery endpoint, and the authorization, token, logout, JWKS, and any other endpoints advertised in the discovery endpoint metadata.
- You need the **VcIdentityProviders** > **Manage** privilege to create, update, or delete a vCenter Server Identity Provider that is required for federated authentication. To limit a user to view the Identity Provider configuration information only, assign the **VcIdentityProviders** > **Read** privilege.

vCenter Server supports only one configured external identity provider (one source), and the vsphere.local identity source. You cannot use multiple external identity providers. vCenter Server Identity Provider Federation uses OpenID Connect (OIDC) for user login to vCenter Server.

This task describes how to add an AD FS group to the vSphere Administrators group as the way to control permissions. You can also configure privileges using AD FS Authorization through global or object permissions in vCenter Server. See the *vSphere Security* documentation for details about adding permissions.

CAUTION:

If you use an Active Directory identity source that you previously added to vCenter Server for your AD FS identity source, do not delete that existing identity source from vCenter Server. Doing so causes a regression with previously assigned roles and group memberships. Both the AD FS user with global permissions and users that were added to the Administrators group will not be able to log in.

Workaround: If you do not need the previously assigned roles and group memberships, and want to remove the previous Active Directory identity source, remove the identity source before creating the AD FS provider and configuring group memberships in vCenter Server.

1. Log in with the vSphere Client to the vCenter Server.
2. Add your AD FS server certificate (or a CA or intermediate certificate that signed the AD FS server certificate) to the Trusted Root Certificates Store.
   a) Navigate to **Administration** > **Certificates** > **Certificate Management**.
   b) Next to **Trusted Root Store**, click **Add**.
   c) Browse for the AD FS certificate and click **Add**.

      The certificate is added in a panel under **Trusted Root Certificates**.
3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Select the **Identity Provider** tab and obtain the Redirect URIs.
   a) Click the informational “i” **icon** next to the “Change identity provider” link.

      Two Redirect URIs are displayed in the pop-up banner.
   b) Copy both URIs to a file or write them down for later use in subsequent steps to configure the AD FS server.
   c) Close the pop-up banner.
5. Create an OpenID Connect configuration in AD FS and configure it for vCenter Server.

   To establish a relying party trust between vCenter Server and an identity provider, you must establish the identifying information and a shared secret between them. In AD FS, you do so by creating an OpenID Connect configuration known as an Application Group, which consists of a Server application and a Web API. The two components specify

the information that vCenter Server uses to trust and communicate with the AD FS server. To enable OpenID Connect in AD FS, see the VMware knowledge base article at https://kb.vmware.com/s/article/78029.

Note the following when you create the AD FS Application Group.

- You need the two Redirect URIs you obtained and saved from the prior step.
- Copy the following information to a file or write it down for use when configuring the vCenter Server Identity Provider in the next step.
  - Client Identifier
  - Shared secret
  - OpenID address of the AD FS server

6. Create an identity provider on vCenter Server.
   a) Return to the **Identity Provider** tab in the vSphere Client.
   b) Click the "Change identity provider" link.
      The Configure Main Identity Provider wizard opens.
   c) Select **Microsoft ADFS** and click **Next**.
      Enter the information that you have gathered previously for the following text boxes:
      - Client Identifier
      - Shared Secret
      - OpenID Address of the AD FS server
   d) Click **Next**.
   e) Enter user and group information for the Active Directory over LDAP connection to search for users and groups.
      vCenter Server derives the AD domain to use for authorization and permissions from the Base Distinguished Name for users. You can add permissions on vSphere objects only for users and groups from this AD domain. Users or groups from AD child domains or other domains in the AD forest are not supported by vCenter Server Identity Provider Federation.

Option	Description
Base distinguished name for users	Base Distinguished Name for users.
Base distinguished name for groups	The base Distinguished Name for groups.
Username	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups.
Password	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups.
Primary server URL	Primary domain controller LDAP server for the domain. Use the format `ldap://hostname:port` or `ldaps://hostname:port`. The port is typically 389 for LDAP connections and 636 for LDAPS connections. For Active Directory multi-domain controller deployments, the port is typically 3268 for LDAP and 3269 for LDAPS. A certificate that establishes trust for the LDAPS endpoint of the Active Directory server is required when you use `ldaps://` in the primary or secondary LDAP URL.
Secondary server URL	Address of a secondary domain controller LDAP server that is used for failover.

Option	Description
SSL certificates	If you want to use LDAPS with your Active Directory LDAP Server or OpenLDAP Server identity source, click `Browse` to select a certificate.

f) Click **Next**, review the information, and click **Finish**.

7. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
8. Configure group membership vCenter Server for AD FS Authorization.
   a) Click the **Groups** tab.
   b) Click the **Administrators** group and click **Add Members**.
   c) Select the domain from the drop-down menu.
   d) In the text box below the drop-down menu, enter the first few characters of AD FS group that you want to add then wait for the drop-down selection to appear.

      It might take several seconds for the selection to appear as vCenter Server establishes the connection to and searches Active Directory.
   e) Select the AD FS group and add it to the Administrators group.
   f) Click **Save**.
9. Verify logging in to vCenter Server with an Active Directory user.

Understanding vCenter Single Sign-On

If you are not using an external identity provider, you must understand the underlying architecture of the built-in identity provider, vCenter Single Sign-On, and how it affects installation and upgrades.

vCenter Single Sign-On Components

vCenter Single Sign-On includes the Security Token Service (STS), an administration server, the vCenter Lookup Service, and the VMware Directory Service (vmdir). The VMware Directory Service is also used for certificate management.

During installation, the following components are deployed as part of a vCenter Server deployment.

STS (Security Token Service)

The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in one of the identity source types supported by vCenter Server. The SAML tokens allow interactive, scripted, and service users (including solution users) who authenticate successfully to vCenter Single Sign-On to use any vCenter service that vCenter Single Sign-On supports without authenticating again to each service.

The vCenter Single Sign-On service signs all tokens with a signing certificate, and stores the token signing certificate on disk. The certificate for the service itself is also stored on disk.

Administration server

The administration server allows users with administrator privileges to vCenter Single Sign-On to configure the vCenter Single Sign-On server and manage users and groups from the vSphere Client. Initially, only the user administrator@*`your_domain_name`* has these privileges. You can change the vSphere domain when you install vCenter Server. Do not name the domain name with your Microsoft Active Directory or OpenLDAP domain name.

VMware Directory Service (vmdir)	A VMware Directory Service (vmdir) is associated with the domain you specify during installation and is included in each vCenter Server deployment. This service is a multi-tenanted, peer-replicating directory service that makes an LDAP directory available on port 389. It also stores and manages vCenter Single Sign-On user accounts and passwords, which are secured by the SHA-512 hashing algorithm. If your environment includes multiple instances of vCenter Server configured in linked mode, an update of vmdir content in one vmdir instance is propagated to all other instances of vmdir. The VMware Directory Service stores not only vCenter Single Sign-On information but also certificate information.
Identity Management Service	Handles identity sources and STS authentication requests.

Using vCenter Single Sign-On with vSphere

When a user logs in to a vSphere component, or when a vCenter Server solution user accesses another vCenter Server service, vCenter Single Sign-On performs authentication. Users must be authenticated with vCenter Single Sign-On and have the necessary privileges for interacting with vSphere objects.

vCenter Single Sign-On authenticates both solution users and other users.

- Solution users represent a set of services in your vSphere environment. During installation, VMCA assigns a certificate to each solution user by default. The solution user uses that certificate to authenticate to vCenter Single Sign-On. vCenter Single Sign-On gives the solution user a SAML token, and the solution user can then interact with other services in the environment.
- When other users log in to the environment, for example, from the vSphere Client, vCenter Single Sign-On prompts for a user name and password. If vCenter Single Sign-On finds a user with those credentials in the corresponding identity source, it assigns the user a SAML token. The user can now access other services in the environment without being prompted to authenticate again.
  Which objects the user can view, and what a user can do, is usually determined by vCenter Server permission settings. vCenter Server administrators assign those permissions from the **Permissions** interface in the vSphere Client, not through vCenter Single Sign-On. See the *vSphere Security* documentation.

vCenter Single Sign-On and vCenter Server Users

Users authenticate to vCenter Single Sign-On by entering their credentials on the login page. After connecting to vCenter Server, authenticated users can view all vCenter Server instances or other vSphere objects for which their role gives them privileges. No further authentication is required.

vCenter Single Sign-On Administrator Users

The vCenter Single Sign-On administrative interface is accessible from the vSphere Client.

To configure vCenter Single Sign-On and manage vCenter Single Sign-On users and groups, the user administrator@vsphere.local or a user in the vCenter Single Sign-On Administrators group must log in to the vSphere Client. Upon authentication, that user can access the vCenter Single Sign-On administration interface from the vSphere Client and manage identity sources and default domains, specify password policies, and perform other administrative tasks.

Groups in the vCenter Single Sign-On Domain

The vCenter Single Sign-On domain (vsphere.local by default) includes several predefined groups. Add users to one of those groups to enable them to perform the corresponding actions.

See Managing vCenter Single Sign-On Users and Groups.

For all objects in the vCenter Server hierarchy, you can assign permissions by pairing a user and a role with the object. For example, you can select a resource pool and give a group of users read privileges to that resource pool object by giving them the corresponding role.

For some services that are not managed by vCenter Server directly, membership in one of the vCenter Single Sign-On groups determines the privileges. For example, a user who is a member of the Administrators group can manage vCenter Single Sign-On. A user who is a member of the CAAdmins group can manage the VMware Certificate Authority, and a user who is in the LicenseService.Administrators group can manage licenses.

The following groups are predefined in vsphere.local. Many of these groups are internal to vsphere.local or give users high-level administrative privileges. Add users to any of these groups only after careful consideration of the risks.

CAUTION: Do not delete any of the predefined groups in the vsphere.local domain. If you do, errors with authentication or certificate provisioning might result.

Table 111: Groups in the vsphere.local Domain

Privilege	Description
Users	Users in the vCenter Single Sign-On domain (vsphere.local by default).
SolutionUsers	Solution users group for vCenter services. Each solution user authenticates individually to vCenter Single Sign-On with a certificate. By default, VMCA provisions solution users with certificates. Do not add members to this group explicitly.
CAAdmins	Members of the CAAdmins group have administrator privileges for VMCA. Do not add members to this group unless you have compelling reasons.
DCAdmins	Members of the DCAdmins group can perform Domain Controller Administrator actions on VMware Directory Service. **Note:** Do not manage the domain controller directly. Instead, use the `vmdir` CLI or the vSphere Client to perform corresponding tasks.
SystemConfiguration.BashShellAdministrators	A user in this group has full access to all the Appliance Management APIs. By default, a user who connects to the vCenter Server with SSH can access only commands in the restricted shell, but users in this group have Bash Shell Access over SSH and gain full privileges similar to the root user.
ActAsUsers	Members of Act-As Users are allowed to get Act-As tokens from vCenter Single Sign-On.
ExternalIDPUsers	This internal group is not used by vSphere. VMware vCloud Air requires this group.
SystemConfiguration.Administrators	Members of the SystemConfiguration.Administrators group can view and manage the system configuration in the vCenter Server Management Interface running on port 5480. These users can view services, start and restart services, and troubleshoot services. These users can also access Appliance Management APIs except for those APIs that modify critical system configurations.
DCClients	This group is used internally to allow the management node access to data in VMware Directory Service. **Note:** Do not modify this group. Any changes might compromise your certificate infrastructure.
ComponentManager.Administrators	Members of the ComponentManager.Administrators group can invoke component manager APIs that register or unregister services, that is, modify services. Membership in this group is not necessary for read access on the services.
LicenseService.Administrators	Members of LicenseService.Administrators have full write access to all licensing-related data and can add, remove, assign, and unassign serial keys for all product assets registered in the licensing service.

Privilege	Description
Administrators	Administrators of the VMware Directory Service (vmdir). Members of this group can perform vCenter Single Sign-On administration tasks. Do not add members to this group unless you have compelling reasons and understand the consequences.
TrustedAdmins	Members of this group can perform VMware®vSphere Trust Authority™ configuration and administration tasks. By default, this group does not contain any members. You must add a member to this group so that you can perform vSphere Trust Authority tasks.
AutoUpdate	This group is used internally for vCenter Cloud Gateway.
SyncUsers	This group is used internally for vCenter Cloud Gateway.
vSphereClientSolutionUsers	This group is used internally for the vSphere Client.
ServiceProviderUsers	Members of this group can manage the vSphere with Tanzu and VMware Cloud on AWS infrastructure.
NsxAdministrators	This group is used for NSX.
WorkloadStorage	Workload storage group.
RegistryAdministrators	Members of this group can manage the registry.
NsxAuditors	This group is used for NSX.
NsxViAdministrators	This group is used for NSX.
SystemConfiguration.SupportUsers	Members of the SystemConfiguration.SupportUsers group can access the support bundle API.
SystemConfiguration.ReadOnly	Members of this group can access vCenter Server Appliance read-only operations under Appliance Management.
VCLSAdmin	Members of this group have administrative privileges for vSphere Cluster Services (vCLS).
AnalyticsService.Administrators	This group is used for the VMware Analytics Service APIs.
vStatsGroup	This group is used for vStats collection.

Configuring vCenter Single Sign-On Identity Sources

When a user logs in with just a user name, vCenter Single Sign-On checks in the default identity source whether that user can authenticate. When a user logs in and includes the domain name in the login screen, vCenter Single Sign-On checks the specified domain if that domain has been added as an identity source. You can add identity sources, remove identity sources, and change the default.

Identity Sources for vCenter Server with vCenter Single Sign-On

You can use identity sources to attach one or more domains to vCenter Single Sign-On. A domain is a repository for users and groups that the vCenter Single Sign-On server can use for user authentication.

Note: At any time, only one default domain exists. If a user from a non-default domain logs in, that user must add the domain name to authenticate successfully. The domain name is in the form:

```
DOMAIN\user
```

The following identity sources are available.

- Active Directory over LDAP. vCenter Single Sign-On supports multiple Active Directory over LDAP identity sources.
- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources.

Note: A future update to Microsoft Windows will change the default behavior of Active Directory to require strong authentication and encryption. This change will impact how vCenter Server authenticates to Active Directory. If you use Active Directory as your identity source for vCenter Server, you must plan to enable LDAPS. For more information about

this Microsoft security update, see https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 and https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Set the Default Domain for vCenter Single Sign-On

Each vCenter Single Sign-On identity source is associated with a domain. vCenter Single Sign-On uses the default domain to authenticate a user who logs in without a domain name. Users who belong to a domain that is not the default domain must include the domain name when they log in.

When a user logs in to a vCenter Server system from the vSphere Client, the login behavior depends on whether the user is in the domain that is set as the default identity source.

- Users who are in the default domain can log in with their user name and password.
- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1
  - Including the domain, for example, user1@mydomain.com
- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Under the **Identity Provider** tab, click **Identity Sources**, select an identity source, and click **Set as Default**.
5. Click **OK**.

   In the domain display, the default domain shows (default) in the Type column.

Add or Edit a vCenter Single Sign-On Identity Source

Users can log in to vCenter Server only if they are in a domain that has been added as a vCenter Single Sign-On identity source. vCenter Single Sign-On administrator users can add identity sources, or change the settings for identity sources that they added.

If you are adding an Active Directory (Integrated Windows Authentication) identity source, the vCenter Server must be in the Active Directory domain. See Add a vCenter Server to an Active Directory Domain.

An identity source can be an Active Directory over LDAP, a native Active Directory (Integrated Windows Authentication) domain, or an OpenLDAP directory service. See Identity Sources for vCenter Server with vCenter Single Sign-On.

Immediately after installation, the vsphere.local domain (or the domain you specified during installation) with the vCenter Single Sign-On internal users is available.

Note:

If you have updated or replaced your Active Directory SSL certificate, you must remove and re-add the identity source in vCenter Server.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Click **Add**.

Initially, each user is assigned the No Access role. A vCenter Server administrator must assign the user at least to the Read Only role before the user can log in. See the topic on using roles to assign privileges in the *vSphere Security* documentation.

Active Directory over LDAP and OpenLDAP Server Identity Source Settings

The Active Directory over LDAP identity source is preferred over the Active Directory (Integrated Windows Authentication) option. The OpenLDAP Server identity source is available for environments that use OpenLDAP.

If you are configuring an OpenLDAP identity source, see the VMware knowledge base article at https://kb.vmware.com/s/article/2064977 for additional requirements.

Important: Groups in AD-over-LDAP identity sources cannot use users in different domains even if you create an additional identity source for each domain.

Groups in LDAP identity sources only recognize those users that exist in the specified user base DN. This can lead to unexpected problems in large Active Directory environments with child domains. For example, consider the following scenario:

1. An Active Directory forest with two child domains, ChildA and ChildB.
2. A vCenter Server configured with two AD-over-LDAP identity sources, one for child domain ChildA and one for child domain ChildB.
3. ChildA contains two users named UserA1 and UserA2.
4. ChildB contains two users named UserB1 and UserB2.

The vCenter Server administrator creates a group in ChildA named TestGroup that contains UserA1, UserA2, UserB1, and UserB2. The vCenter Server administrator grants login (or any) privileges to TestGroup. Unfortunately, UserB1 and UserB2 cannot log in because they reside in a different domain than the group.

As a workaround, perform the following:

1. Create another group named SecondTestGroup in ChildB.
2. Remove UserB1 and UserB2 from TestGroup.
3. Add UserB1 and UserB2 to SecondTestGroup.
4. In vCenter Server, assign SecondTestGroup the same privileges that were granted to TestGroup.

Note: Microsoft Windows has changed the default behavior of Active Directory to require strong authentication and encryption. This change impacts how vCenter Server authenticates to Active Directory. If you use Active Directory as your identity source for vCenter Server, you must enable LDAPS. For more information about this Microsoft security update, see https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 and https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Table 112: Active Directory over LDAP and OpenLDAP Server Settings

Option	Description
Name	Name of the identity source.
Base DN for users	Base Distinguished Name for users. Enter the DN from which to start user searches. For example, cn=Users,dc=myCorp,dc=com.
Base DN for groups	The Base Distinguished Name for groups. Enter the DN from which to start group searches. For example, cn=Groups,dc=myCorp,dc=com.
Domain name	The FQDN of the domain.
Domain alias	For Active Directory identity sources, the domain's NetBIOS name. Add the NetBIOS name of the Active Directory domain as an alias of the identity source if you are using SSPI authentications. For OpenLDAP identity sources, the domain name in capital letters is added if you do not specify an alias.
User name	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups. The ID can be in any of these formats: • UPN (user@domain.com) • NetBIOS (DOMAIN\user) • DN (cn=user,cn=Users,dc=domain,dc=com) The user name must be fully-qualified. An entry of "user" does not work.
Password	Password of the user who is specified by **Username**.
Connect to	Domain controller to connect to. Can be any domain controller in the domain, or specific controllers.
Primary Server URL	Primary domain controller LDAP server for the domain. You can use either the host name or the IP address. Use the format `ldap://hostname_or_IPaddress:port` or `ldaps://hostname_or_IPaddress:port`. The port is typically 389 for LDAP connections and 636 for LDAPS connections. For Active Directory multi-domain controller deployments, the port is typically 3268 for LDAP and 3269 for LDAPS. A certificate that establishes trust for the LDAPS endpoint of the Active Directory server is required when you use `ldaps://` in the primary or the secondary LDAP URL.
Secondary server URL	Address of a secondary domain controller LDAP server that is used when the primary domain controller is unavailable. You can use either the host name or the IP address. For every LDAP operation, vCenter Server always tries the primary domain controller before falling back to the secondary domain controller. This can lead to Active Directory logins taking some time, and even failing, when the primary domain controller is unavailable. **Note:** When the primary domain controller fails, the secondary domain controller might not take over automatically.

Option	Description
Certificates (for LDAPS)	If you want to use LDAPS with your Active Directory LDAP Server or OpenLDAP Server identity source, click `Browse` to select a certificate that was exported from the domain controller specified in the LDAPS URL. (Note that the certificate used here is not a root CA certificate.) To export the certificate from Active Directory, consult the Microsoft documentation. You can browse for and select multiple certificates. **Tip:** When browsing for and selecting multiple certificates, they must be located in the same directory. vCenter Server only trusts certificates directly signed by a registered and trusted certificate authority. vCenter Server does not trace a path up to a registered CA certificate and only checks if the certificate is signed by a registered and trusted certificate authority. As long as your certificate is signed by a publicly trusted certificate authority, or is self-signed, no further action is necessary. However, if you create your own internal certificates (that is, you use a private certificate authority), you might need to include those certificates. For example, if your organization uses Microsoft Enterprise Root Certificate Authority to generate the LDAPS certificate, you must also select the Enterprise Root Certificate to add it to vCenter Server. In addition, if you use intermediate certificate authorities between the LDAPS certificate and the Enterprise Root certificate, you must also select those intermediate certificates to add them to vCenter Server.

Active Directory Identity Source Settings

If you select the Active Directory (Integrated Windows Authentication) identity source type, you can use the local machine account as your SPN (Service Principal Name) or specify an SPN explicitly. You can use this option only if the vCenter Single Sign-On server is joined to an Active Directory domain.

Prerequisites for Using an Active Directory (Integrated Windows Authentication) Identity Source

You can set up vCenter Single Sign-On to use an Active Directory (Integrated Windows Authentication) identity source only if that identity source is available. Follow the instructions in the *vCenter Server Configuration* documentation.

Note: Active Directory (Integrated Windows Authentication) always uses the root of the Active Directory domain forest. To configure your Integrated Windows Authentication identity source with a child domain within your Active Directory forest, see the VMware knowledge base article at http://kb.vmware.com/kb/2070433.

Select **Use machine account** to speed up configuration. If you expect to rename the local machine on which vCenter Single Sign-On runs, specifying an SPN explicitly is preferable.

If you have enabled diagnostic event logging in your Active Directory to identify where hardening might be needed, you might see a log event with Event ID 2889 on that directory server. Event ID 2889 is generated as an anomaly rather than a security risk when using Integrated Windows Authentication. For more information about Event ID 2889, see the VMware knowledge base article at https://kb.vmware.com/s/article/78644.

Table 113: Add Identity Source Settings

Text Box	Description
Domain name	FQDN of the domain name, for example, mydomain.com. Do not provide an IP address. This domain name must be DNS-resolvable by the vCenter Server system.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.
Use Service Principal Name (SPN)	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service Principal Name (SPN)	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, `STS/example.com`. The SPN must be unique across the domain. Running the `setspn -S` command checks that no duplicate is created. See the Microsoft documentation for information on `setspn`.
User Principal Name (UPN) **Password**	Name and password of a user who can authenticate with this identity source. Use the email address format, for example, `jchin@mydomain.com`. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).

Add or Remove an Identity Source Using the CLI

You can use the `sso-config` utility to add or remove an identity source.

If you are adding an Active Directory identity source, the vCenter Server must be in the Active Directory domain. See Add a vCenter Server to an Active Directory Domain.

Enable SSH login. See Manage vCenter Server from the vCenter Server Shell.

An identity source can be a native Active Directory (Integrated Windows Authentication) domain, AD over LDAP, AD over LDAP using LDAPS (LDAP over SSL), or OpenLDAP. See Identity Sources for vCenter Server with vCenter Single Sign-On. You also use the `sso-config` utility to set up smart card and RSA SecurID authentication.

1. Use SSH or another remote console connection to start a session on the vCenter Server system.
2. Log in as root.
3. Change to the directory where the `sso-config` utility is located.

   ```
   cd /opt/vmware/bin
   ```

4. Refer to the `sso-config` help by running `sso-config.sh -help` , or see the VMware knowledge base article at https://kb.vmware.com/s/article/67304 for usage examples.

Use vCenter Single Sign-On with Windows Session Authentication

You can use vCenter Single Sign-On with Windows Session Authentication (SSPI). You must join the vCenter Server to an Active Directory domain before you can use SSPI.

- Join the vCenter Server to an Active Directory domain. See Add a vCenter Server to an Active Directory Domain.
- Verify that the domain is set up properly. See the VMware knowledge base article at http://kb.vmware.com/kb/2064250.
- Verify that the Enhanced Authentication Plug-In is installed. See *vCenter Server Installation and Setup*.

Note: When you configure vCenter Server to use federated authentication with Active Directory Federation Services, the Enhanced Authentication Plug-in only applies to configurations where vCenter Server is the identity provider (Active Directory over LDAP, Integrated Windows Authentication, and OpenLDAP configurations).

1. Navigate to the vSphere Client login page.
2. Select the **Use Windows session authentication** check box.
3. Log in using the Active Directory user name and password.
   - If the Active Directory domain is the default identity source, log in with your user name, for example jlee.
   - Otherwise, include the domain name, for example, jlee@example.com.

Managing the vCenter Server Security Token Service

The vCenter Server Security Token Service (STS) is a Web service that issues, validates, and renews security tokens.

As a token issuer, the Security Token Service (STS) uses a private key to sign the tokens and publishes the public certificates for services to verify the token signature. vCenter Server manages the STS signing certificates and stores them in the VMware Directory Service (vmdir). Tokens can have a significant lifetime, and historically might have been signed by any one of multiple keys.

Users present their primary credentials to the STS interface to acquire tokens. The primary credential depends on the type of user.

Solution user	Valid certificate.
Other users	User name and password available in a vCenter Single Sign-On identity source.

STS authenticates the user based on the primary credentials, and constructs a SAML token that contains user attributes.

By default, the VMware Certificate Authority (VMCA) generates the STS signing certificate. You can refresh the STS signing certificate with a new VMCA certificate. You can also import and replace the default STS signing certificate with a custom or third-party generated STS signing certificate. Do not replace the STS signing certificate unless the security policy of your company requires replacing all certificates.

You can use the vSphere Client to:

- Refresh STS certificates
- Import and replace custom and third-party generated STS certificates
- View STS certificate details, such as the expiration date

You can also use the command line to replace custom and third-party generated STS certificates.

STS Certificate Duration and Expiration

A fresh installation of vSphere 7.0 Update 1 and later creates an STS signing certificate with a duration of 10 years. When an STS signing certificate is close to expiring, an alarm warns you starting at 90 days once per week, and then daily when seven days away.

Note: In certain circumstances, replacing your STS signing certificates can change the duration of the certificates. When performing certificate replacement, pay attention to the issuing and expiration dates.

Refresh a vCenter Server STS Certificate Using the vSphere Client

You can refresh your vCenter Server STS signing certificates using the vSphere Client. The VMware Certificate Authority (VMCA) issues a new certificate and replaces the current certificate.

For certificate management, you must supply the password of the administrator of the local domain (administrator@vsphere.local by default). If you are renewing certificates, you must also supply the vCenter Single Sign-On credentials for a user with administrator privileges on the vCenter Server system.

When you refresh STS signing certificates, the VMware Certificate Authority (VMCA) issues a new certificate and replaces the current certificate in the VMware Directory Service (vmdir). STS starts using the new certificate to issue new tokens. In an Enhanced Linked Mode configuration, vmdir uploads the new certificate from the issuing vCenter Server system to all linked vCenter Server systems. When you refresh STS signing certificates, you must restart the vCenter Server system, and any other vCenter Server system that is part of an Enhanced Linked Mode configuration.

If you are using a custom generated or third-party STS signing certificate, the refresh overwrites that certificate with a VMCA-issued certificate. To update custom generated or third-party STS signing certificates, use the import and replace option. See Import and Replace a vCenter Server STS Certificate Using the vSphere Client.

The VMCA-issued STS signing certificate is valid for 10 years and is not an external-facing certificate. Do not replace this certificate unless the security policy of your company requires it.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@`mydomain`.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under **STS Signing Certificate**, click **Actions** > **Refresh with vCenter certificate**.

   If you are using a custom generated or third-party STS signing certificate, the refresh action overwrites that certificate with a VMCA-generated certificate.

   Note: If you were using third-party certificates for compliance reasons, the refresh might cause your vCenter Server systems to go out of compliance. Also, if you are using a custom generated or third-party STS signing certificate, the Security Token Service no longer uses that custom or third-party certificate for token signing.
6. Click **Refresh**.

   The VMCA refreshes the STS signing certificate on this vCenter Server system and on any linked vCenter Server systems.
7. Optional: If the **Force Refresh** button appears, vCenter Single Sign-On has detected a problem. Before clicking **Force Refresh**, consider the following potential results.
   - If all the impacted vCenter Server systems are not running at least vSphere 7.0 Update 3, they do not support the certificate refresh.
   - Selecting **Force Refresh** requires that you restart all vCenter Server systems and can render those systems inoperable until you do so.

   a) If you are unsure of the impact, click **Cancel** and research your environment.
   b) If you are sure of the impact, click **Force Refresh** to proceed with the refresh then manually restart your vCenter Server systems.

To ensure that all the STS services in an Enhanced Linked Mode configuration validate the new tokens, you must restart the linked vCenter Server systems. See the topic about how to reboot vCenter Server in the *vCenter Server Configuration* documentation.

Import and Replace a vCenter Server STS Certificate Using the vSphere Client

You can import and replace the vCenter Server STS certificate with a custom generated or third-party certificate using the vSphere Client client.

For certificate management, you must supply the password of the administrator of the local domain (administrator@vsphere.local by default). You also must supply the vCenter Single Sign-On credentials for a user with administrator privileges on the vCenter Server system.

To import and replace the default STS signing certificate, you must first generate a new certificate. When you import and replace STS signing certificates, the VMware Directory Service (vmdir) uploads the new certificate from the issuing vCenter Server system to all linked vCenter Server systems.

The STS certificate is not an external-facing certificate. Do not replace this certificate unless the security policy of your company requires it.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under **STS Signing Certificate**, click **Actions** > **Import and Replace**.
6. Select the PEM file.

   The PEM file includes the signing certificate chain and the private key.
7. Click **Replace**.

   The STS signing certificate is replaced on this vCenter Server system and on any linked vCenter Server systems.
8. Restart the vCenter Server system, and any other vCenter Server system that is part of an Enhanced Linked Mode configuration.

   See the topic about how to reboot vCenter Server in the *vCenter Server Configuration* documentation.

Replace a vCenter Server STS Certificate Using the Command Line

You can replace the vCenter Server STS certificate with a custom generated or third-party certificate using the CLI.

Enable SSH login to vCenter Server. See Manage vCenter Server from the vCenter Server Shell.

To use a company required certificate or to refresh a certificate that is near expiration, you can replace the existing STS signing certificate. To replace the default STS signing certificate, you must first generate a new certificate.

The STS certificate is not an external-facing certificate. Do not replace this certificate unless the security policy of your company requires it.

CAUTION: You must use the procedures described here. Do not replace the certificate directly in the file system.

1. Log in to the vCenter Server shell as root.
2. Create a certificate.
   a) Create a top-level directory to hold the new certificate and verify the location of the directory.

```
mkdir newsts
cd newsts
```

```
pwd
#resulting output: /root/newsts
```

b) Copy the `certool.cfg` file into the new directory.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

c) Using a command-line editor such as Vim, open your copy of the `certool.cfg` file and edit it to use the local vCenter Server IP address and hostname. The country is required and has to be two characters, as shown in the following example.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

d) Generate the key.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/sts.key --pub-
key=/root/newsts/sts.pub
```

e) Generate the certificate.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --privkey=/root/new-
sts/sts.key --config=/root/newsts/certool.cfg
```

f) Create a PEM file with the certificate chain and private key.

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3. Update the STS signing certificate, for example:

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

4. Restart the vCenter Server system, and any other vCenter Server system that is part of an Enhanced Linked Mode configuration. See the topic about how to reboot vCenter Server in the *vCenter Server Configuration* documentation.

   For authentication to work correctly, you must restart vCenter Server. Both the STS service and the vSphere Client are restarted.

View the Active vCenter Server STS Signing Certificate Chain

You can use the vSphere Client to view the active vCenter Server STS signing certificate chain.

You can view the following information on the active STS certificate.

- "Valid until" date

- A green check for a valid certificate, and an orange check warning of an expired certificate
- A **View Details** link to show the active certificate chain

1. Log in with the vSphere Client to the vCenter Server.
2. Enter the user name and password for a user that has at least Read privileges.
3. Navigate to the Certificate Management UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. To view details for the active STS certificate, click **View Details**.

Determine the Expiration Date of an LDAPS SSL Certificate

When using Active Directory over LDAPS, you can upload an SSL certificate for the LDAP traffic. SSL certificates expire after a predefined lifespan. You can view the certificate's expiration date so that you know to replace or renew the certificate before it expires.

Enable SSH login to vCenter Server. See Manage vCenter Server from the vCenter Server Shell.

vCenter Server alerts you when an active LDAP SSL certificate is close to its expiration date.

You see certificate expiration information only if you use Active Directory over LDAP or an OpenLDAP identity source and specify an `ldaps://` URL for the server.

1. Log in as root to the vCenter Server.
2. Run the following command.

   ```
   /opt/vmware/bin/sso-config.sh -get_identity_sources
   ```

   Ignore the SLF4J messages.
3. To determine the expiration date, view the SSL certificate's details and verify the `NotAfter` field.

Managing vCenter Single Sign-On Policies

vCenter Single Sign-On policies enforce the security rules for local accounts and tokens in general. You can view and edit the default vCenter Single Sign-On password policy, lockout policy, and token policy.

Edit the vCenter Single Sign-On Password Policy

The vCenter Single Sign-On password policy determines the password format and password expiration. Password policy applies only to users in the vCenter Single Sign-On domain (vsphere.local).

By default, vCenter Single Sign-On built-in user account passwords expire after 90 days. The vSphere Client reminds you when your password is about to expire.

See Change Your vCenter Single Sign-On Password.

Note: The administrator account (administrator@vsphere.local) does not get locked out nor does its password expire. Proper security practice is to audit logins from this account and rotate the password regularly.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Click the **Local Accounts** tab.
5. Click **Edit** for the **Password Policy** row.
6. Edit the password policy.

Option	Description
Description	Password policy description.
Maximum lifetime	Maximum number of days that a password is valid before the user must change it. The maximum number of days you can enter is 999999999. A value of zero (0) means that the password never expires.
Restrict reuse	Number of previous passwords that cannot be reused. For example, if you enter 6, the user cannot reuse any of the last six passwords.
Maximum length	Maximum number of characters that are allowed in the password. The maximum number of characters supported for password is 32. The behaviour is undefined if the minimum and maximum password length is beyond this permissible range.
Minimum length	Minimum number of characters required in the password. The minimum length must be no less than the combined minimum of alphabetic, numeric, and special character requirements. The minimum number of characters supported for password is 8. The behaviour is undefined if the minimum and maximum password length is beyond this permissible range.
Character requirements	Minimum number of different character types that are required in the password. You can specify the number of each type of character, as follows: • Special: & # % • Alphabetic: A b c D • Uppercase: A B C • Lowercase: a b c • Numeric: 1 2 3 • Identical Adjacent: The number must be greater than 0. For example, if you enter 1, the following password is not allowed: p@$$word. The minimum number of alphabetic characters must be no less than the combined uppercase and lowercase characters.

Note: The password policy picks up the maximum length value only if the minimum length is greater than 20 characters. The behavior of the password policy is undefined or could result in failure of services when the minimum length value is greater than 20 characters and the maximum length is set to any value. To avoid a potential problem, leave the minimum length set to the default value of 8 characters, or no greater than 20 characters.

7. Click **Save**.

Edit the vCenter Single Sign-On Lockout Policy

If a user attempts to log in with incorrect credentials, a vCenter Single Sign-On lockout policy specifies when the user's vCenter Single Sign-On account is locked. Administrators can edit the lockout policy.

If a user logs in to vsphere.local multiple times with the wrong password, the user is locked out. The lockout policy allows administrators to specify the maximum number of failed login attempts, and set the time interval between failures. The policy also specifies how much time must elapse before the account is automatically unlocked.

Note: The lockout policy applies only to user accounts, not to system accounts such as administrator@vsphere.local.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Click the **Local Accounts** tab.
5. Click **Edit** for the **Lockout Policy** row.

   You might need to scroll down to see the **Lockout Policy** row.
6. Edit the parameters.

Option	Description
Description	Optional description of the lockout policy.
Maximum number of failed login attempts	Maximum number of failed login attempts that are allowed before the account is locked.
Time interval between failures	Time period in which failed login attempts must occur to trigger a lockout.
Unlock time	Amount of time that the account remains locked. If you enter 0, the administrator must unlock the account explicitly.

7. Click **Save**.

Edit the vCenter Single Sign-On Token Policy

The vCenter Single Sign-On token policy specifies token properties such as the clock tolerance and renewal count. You can edit the token policy to ensure that the token specification conforms to security standards in your corporation.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Click the **Local Accounts** tab.
5. Click **Edit** for the **Token Trustworthiness** row.
   You might need to scroll down to see the **Token Trustworthiness** row.
6. Edit the token policy configuration parameters.

Option	Description
Clock Tolerance	Time difference, in milliseconds, that vCenter Single Sign-On tolerates between a client clock and the domain controller clock. If the time difference is greater than the specified value, vCenter Single Sign-On declares the token invalid.
Maximum Token Renewal Count	Maximum number of times that a token can be renewed. After the maximum number of renewal attempts, a new security token is required.
Maximum Token Delegation Count	Holder-of-key tokens can be delegated to services in the vSphere environment. A service that uses a delegated token performs the service on behalf of the principal that provided the token. A token request specifies a DelegateTo identity. The DelegateTo value can either be a solution token or a reference to a solution token. This value specifies how many times a single holder-of-key token can be delegated.
Maximum Bearer Token Lifetime	Bearer tokens provide authentication based only on possession of the token. Bearer tokens are intended for short-term, single-operation use. A bearer token does not verify the identity of the user or entity that is sending the request. This value specifies the lifetime value of a bearer token before the token has to be reissued.
Maximum Holder-of-Key Token Lifetime	Holder-of-key tokens provide authentication based on security artifacts that are embedded in the token. Holder-of-key tokens can be used for delegation. A client can obtain a holder-of-key token and delegate that token to another entity. The token contains the claims to identify the originator and the delegate. In the vSphere environment, a vCenter Server system obtains delegated tokens on a user's behalf and uses those tokens to perform operations. This value determines the lifetime of a holder-of-key token before the token is marked invalid.

7. Click **Save**.

Edit Password Expiration Notification for Active Directory (Integrated Windows Authentication) Users

The Active Directory password expiration notification is separate from the vCenter Server SSO password expiration. The default password expiration notification for an Active Directory user is 30 days but the actual password expiration depends on your Active Directory system. The vSphere Client controls the expiration notification. You can change the default expiration notification to meet the security standards in your corporation.

- Enable SSH login to vCenter Server. See Manage vCenter Server from the vCenter Server Shell.

1. Log in to the vCenter Server shell as a user with administrator privileges.
   The default user with the super administrator role is root.
2. Change directory to the location of the vSphere Client`webclient.properties` file.
   ```
   cd /etc/vmware/vsphere-ui
   ```
3. Open the `webclient.properties` file with a text editor.
4. Edit the following variable.
   ```
   sso.pending.password.expiration.notification.days = 30
   ```
5. Restart the vSphere Client.
   ```
   service-control --stop vsphere-ui
   service-control --start vsphere-ui
   ```

Managing vCenter Single Sign-On Users and Groups

A vCenter Single Sign-On administrator user can manage users and groups in the vsphere.local domain from the vSphere Client.

The vCenter Single Sign-On administrator user can perform the following tasks.

Add vCenter Single Sign-On Users

Users listed on the **Users** tab in the vSphere Client are internal to vCenter Single Sign-On and belong to the vsphere.local domain. You add users to that domain from one of the vCenter Single Sign-On management interfaces.

You can select other domains and view information about the users in those domains, but you cannot add users to other domains from a vCenter Single Sign-On management interface.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.
   If you specified a different domain during installation, log in as administrator@*`mydomain`*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. If vsphere.local is not the currently selected domain, select it from the drop-down menu.
   You cannot add users to other domains.
5. On the **Users** tab, click **Add**.
6. Enter a user name and password for the new user.
   The maximum number of characters allowed for the user name is 300.
   You cannot change the user name after you create a user. The password must meet the password policy requirements for the system.
7. Optional: Enter the first name and the last name of the new user.
8. Optional: Enter an email address and description for the user.
9. Click **Add**.

When you add a user, that user initially has no privileges to perform management operations.

Add the user to a group in the vsphere.local domain, for example, to the group of users who can administer VMCA (CAAdmins) or to the group of users who can administer vCenter Single Sign-On (Administrators). See Add Members to a vCenter Single Sign-On Group.

Disable and Enable vCenter Single Sign-On Users

When a vCenter Single Sign-On user account is disabled, the user cannot log in to the vCenter Single Sign-On server until an administrator enables the account. You can disable and enable accounts from one of the vCenter Single Sign-On management interfaces.

You must be a member of the vCenter Single Sign-On Administrators group to disable and enable vCenter Single Sign-On users.

Disabled user accounts remain available in the vCenter Single Sign-On system, but the user cannot log in or perform operations on the server. Users with administrator privileges can disable and enable accounts from the vCenter **Users and Groups** page.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. Select a user name, click the vertical ellipsis icon, and click **Disable**.
5. Click **OK**.
6. To enable the user again, click the vertical ellipsis icon, click **Enable**, and click **OK**.

Delete a vCenter Single Sign-On User

You can delete users that are in the vsphere.local domain from a vCenter Single Sign-On management interface. You cannot delete local operating system users or users in another domain from a vCenter Single Sign-On management interface.

CAUTION: If you delete the administrator user in the vsphere.local domain, you can no longer log in to vCenter Single Sign-On. Reinstall vCenter Server and its components.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. Select **Users**, and select the vsphere.local domain from the drop-down menu.
5. In the list of users, select the user that you want to delete and click the vertical ellipsis icon.
6. Click **Delete**.

   Proceed with caution. You cannot undo this action.

Edit a vCenter Single Sign-On User

You can change the password or other details of a vCenter Single Sign-On user from a vCenter Single Sign-On management interface. You cannot rename users in the vsphere.local domain. That means you cannot rename administrator@vsphere.local.

You can create additional users with the same privileges as administrator@vsphere.local.

vCenter Single Sign-On users are stored in the vCenter Single Sign-On vsphere.local domain.

You can review the vCenter Single Sign-On password policies from the vSphere Client. Log in as administrator@vsphere.local and from the **Administration** menu, select **Configuration** > **Local Accounts** > **Password Policy**.

See also Edit the vCenter Single Sign-On Password Policy.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. Click **Users**.
5. Click the vertical ellipsis icon and select **Edit**.
6. Edit the user attributes.

   You cannot change the user name of the user.

   The password must meet the password policy requirements for the system.
7. Click **OK**.

Add a vCenter Single Sign-On Group

The vCenter Single Sign-On**Groups** tab shows groups in the local domain, vsphere.local by default. You add groups if you need a container for group members (principals).

You cannot add groups to other domains, for example, the Active Directory domain, from the vCenter Single Sign-On**Groups** tab.

If you do not add an identity source to vCenter Single Sign-On, creating groups and adding users can help you organize the local domain.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. Select **Groups**, and click **Add Group**.
5. Enter a name and description for the group.
   The maximum number of characters allowed for the group name is 300. You cannot change the group name after you create the group.
6. From the **Add Members** drop-down menu, select the identity source that contains the member to add to the group.
   If you have configured an external identity provider such as AD FS, the domain of that identity provider is available to select in the **Add Members** drop-down menu.
7. Enter a search term.
8. Select the member.
   You can add more than one member.
9. Click **Add**.

See Add Members to a vCenter Single Sign-On Group.

Add Members to a vCenter Single Sign-On Group

Members of a vCenter Single Sign-On group can be users or other groups from one or more identity sources. You can add new members from the vSphere Client.

See the VMware knowledge base article at http://kb.vmware.com/kb/2095342 for the background information.

Groups listed on the **Groups** tab in the Web interface are part of the vsphere.local domain. See Groups in the vCenter Single Sign-On Domain.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.
   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. Click **Groups** and click the group (for example, Administrators).
5. From the **Add Members** drop-down menu, select the identity source that contains the member to add to the group.
   If you have configured an external identity provider, such as AD FS, the domain of that identity provider is available to select in the **Add Members** drop-down menu.
6. Enter a search term.
7. Select the member.
   You can add more than one member.

8. Click **Save**.

Remove Members from a vCenter Single Sign-On Group

You can remove members from a vCenter Single Sign-On group by using the vSphere Client. When you remove a member (user or group) from a group, you do not delete the member from the system.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Users and Groups**.
4. Select **Groups** and click a group.
5. In the list of group members, select the user or group that you want to remove and click the vertical ellipsis icon.
6. Click **Remove Member**.
7. Click **Remove**.

The user is removed from the group, but is still available in the system.

Change Your vCenter Single Sign-On Password

Users in the local domain, vsphere.local by default, can change their vCenter Single Sign-On passwords from the vSphere Client. Users in other domains change their passwords following the rules for that domain.

The vCenter Single Sign-On lockout policy determines when your password expires. By default, vCenter Single Sign-On passwords expire after 90 days, but administrator passwords such as the password for administrator@vsphere.local do not expire. vCenter Single Sign-On management interfaces show a warning when your password is about to expire.

Note: You can change a password only if it is not expired.

If the password is expired, the administrator of the local domain, administrator@vsphere.local by default, can reset the password by using the `dir-cli password reset` command. Only members of the Administrator group for the vCenter Single Sign-On domain can reset passwords.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. In the upper navigation pane, to the right of the Help menu, click your user name to pull down the menu.

   As an alternative, you can select **Single Sign On** > **Users and Groups** and select **Edit** from the vertical ellipsis menu.
4. Enter your current password.
5. Enter a new password and confirm it.

   The password must conform to the password policy.

6. Click **Save**.

Understanding Other Authentication Options

Starting with vSphere 7.0, external identity provider federation is the preferred authentication method for vCenter Server. You can still authenticate by using Windows session Authentication (SSPI), by using a smart card (UPN-based Common Access Card or CAC), or by using an RSA SecurID token.

Two-Factor Authentication Methods

The two-factor authentication methods are often required by government agencies or large enterprises.

External Identity Provider Federation	External identity provider federation enables you to use the authentication mechanisms supported by the external identity provider, including multi-factor authentication.
Smart Card Authentication	Smart card authentication allows access only to users who attach a physical card reader to the computer that they log in to. An example is Common Access Card (CAC) authentication. The administrator can deploy the PKI so that the smart card certificates are the only client certificates that the CA issues. For such deployments, only smart card certificates are presented to the user. The user selects a certificate, and is prompted for a PIN. Only users who have both the physical card and the PIN that matches the certificate can log in.
RSA SecurID Authentication	For RSA SecurID authentication, your environment must include a correctly configured RSA Authentication Manager. If the vCenter Server is configured to point to the RSA server, and if RSA SecurID Authentication is enabled, users can log in with their user name and token. See the two vSphere Blog posts about RSA SecurID setup for details. **Note:** vCenter Single Sign-On supports only native SecurID. It does not support RADIUS authentication.

Specifying a Nondefault Authentication Method

Administrators can set up a nondefault authentication method from the vSphere Client, or by using the `sso-config` script.

- For smart card authentication, you can perform the vCenter Single Sign-On setup from the vSphere Client or by using `sso-config`. Setup includes enabling smart card authentication and configuring certificate revocation policies.
- For RSA SecurID, you use the `sso-config` script to configure RSA Authentication Manager for the domain, and to enable RSA token authentication. You cannot configure RSA SecurID authentication from the vSphere Client. However, if you enable RSA SecurID, that authentication method appears in the vSphere Client.

Combining Authentication Methods

You can enable or disable each authentication method separately by using `sso-config`. Leave user name and password authentication enabled initially, while you are testing a two-factor authentication method, and set only one authentication method to enabled after testing.

Smart Card Authentication Login

A smart card is a small plastic card with an embedded integrated circuit chip. Many government agencies and large enterprises use smart cards such as Common Access Card (CAC) to increase the security of their systems and to comply with security regulations. A smart card is used in environments where each machine includes a smart card reader. Smart card hardware drivers that manage the smart card are typically preinstalled.

Note: In vSphere 7.0 Update 2 and later, you can enable FIPS on vCenter Server. See the *vSphere Security* documentation. RSA SecureID and CAC authentication are not supported when FIPS is enabled. Use external identity provider federation for MFA authentication. See Configuring vCenter Server Identity Provider Federation.

Users who log in to a vCenter Server system are prompted to authenticate with a smart card and PIN combination, as follows.

1. When a user inserts the smart card into the smart card reader, the browser reads the certificates on the card.
2. The browser prompts the user to select a certificate, then prompts the user for the PIN for that certificate.
3. vCenter Single Sign-On checks whether the certificate on the smart card is known. If revocation checking is turned on, vCenter Single Sign-On also checks whether the certificate is revoked.
4. If the certificate is known to vCenter Single Sign-On, and is not a revoked certificate, the user is authenticated and can perform tasks for which that the user has permissions.

Note: It usually makes sense to leave user name and password authentication enabled during testing. After testing is complete, deactivate user name and password authentication and activate smart card authentication. Subsequently, the vSphere Client allows only smart card login. Only users with root or administrator privileges on the machine can reactivate user name and password authentication by logging in to the vCenter Server directly.

Configuring and Using Smart Card Authentication

You can set up your environment to require smart card authentication when a user connects to a vCenter Server from the vSphere Client.

Configuring smart card authentication involves the following high-level steps:

1. Configuring the vCenter Server system to request client certificates.
2. Activating the smart card configuration.
   You can use either the vSphere Client or the `sso-config` utility to activate the configuration.
3. Customizing certificate revocation checking.
   You can use either the vSphere Client or the `sso-config` utility to customize the checking.

Configure vCenter Server Smart Card Authentication to Request Client Certificates

Before you enable smart card authentication, you must create a trusted client CA store and potentially configure the reverse proxy on the vCenter Server system.

Copy the certificate authority (CA) certificates to the vCenter Server system to use to create the trusted client CA store. This store must contain the trusted certificates issued by the CA for the client certificate. The client here is the browser from which the smart card process prompts the end user for information.

Note: vCenter Server 7.0 supports the HTTP/2 protocol. All modern browsers and applications, including the vSphere Client, connect to vCenter Server using HTTP/2. However, smart card authentication requires use of the HTTP/1.1 protocol. Enabling smart card authentication disables Application-Layer Protocol Negotiation (ALPN, https://tools.ietf.org/html/rfc7301) for HTTP/2, effectively preventing the browser from using HTTP/2. Applications that use only HTTP/2, without relying on ALPN, continue to work.

To complete smart card authentication, clients must be permitted access to port 3128/TCP on the appropriate vCenter Server. Check your perimeter firewalls to ensure that access has been granted.

The connection is redirected to port 3128 during smart card login. Port 3128 only supports pre-configured mutual authentication connections and it is not intended as a direct browser endpoint. It does not return an HSTS header. If your vulnerability scanner reports this behavior, it can be safely ignored.

Reverse proxy configuration is required in vSphere 7.0 through vSphere 7.0 Update 3h. Starting with vSphere 7.0 Update 3i, you no longer need to configure the reverse proxy (Step 5).

The configuration uses port 3128, which is set and opened automatically on vCenter Server (as of vSphere 7.0 Update 3i).

1. Log in to the vCenter Server shell as the root user.
2. Create a trusted client CA store on the vCenter Server using the exact path and PEM name, `/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`.

   Warning: You must use the exact path and PEM name, `/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`.

   a) Change to the `/usr/lib/vmware-sso/` directory.

   ```
   cd /usr/lib/vmware-sso/
   ```

   b) To create the trusted client CA store, run the `openssl` command, taking as input your trusted signing certificate. For example, the following command creates the `clienttrustCA.pem` file from the `xyzCompanySmartCardSigningCA.cer` trusted signing certificate.

   ```
   openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
   ```

   You can add additional certificates to the trusted client CA store by running the `openssl` command with the ">>" operator to append the additional certificate. For example, the following command appends `xyzCompanySmartCardSigningCA2.cer` to the existing `clienttrustCA.pem` file.

   ```
   openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA2.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
   ```

3. To validate that the contents of the `clienttrustCA.pem` file contain the trusted CAs that signed the smart card certificates, run the `keytool` command.

   For example:

   ```
   keytool -printcert -file /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem | grep -i "owner\|sha1\|issuer:\|valid"
   ```

4. Verify that the CA names match the Smart Card User Certificate Chain.

   For example, you can run the following command.

   ```
   sso-config.sh -get_authn_policy -t vsphere.local | grep trusted
   ```

   The root and intermediate certificates must have matching thumbprints, names, valid dates, and so on.

   Note: You can also use the vSphere Client (**Single Sign On** > **Configuration** > **Smart Card Configuration** > **Smart Card Authentication** > **Trusted CA Certificates**).

5. For vSphere versions prior to 7.0 Update 3i, make a backup of the `/etc/vmware-rhttpproxy/config.xml` file that includes the reverse proxy definition, open `config.xml` in an editor, and make and save the following changes.

   ```
   <http>
   <maxConnections> 2048 </maxConnections>
   <requestClientCertificate>true</requestClientCertificate>
   <clientCertificateMaxSize>4096</clientCertificateMaxSize>
   <clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
   </http>
   ```

   The `config.xml` file includes some of these elements. Uncomment, update, or add the elements as needed.

   Note: This step is no longer necessary starting with vSphere 7.0 Update 3i.

6. Restart the appropriate service.

vSphere Version	Action
Prior to 7.0 Update 3i	Restart the reverse proxy service. `/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy`
7.0 Update 3i and later	Restart the STS service. `/usr/lib/vmware-vmon/vmon-cli --restart sts`

Use the vSphere Client to Manage Smart Card Authentication

You can enable and disable smart card authentication, customize the login banner, and set up the revocation policy from the vSphere Client.

- Verify that an enterprise Public Key Infrastructure (PKI) is set up in your environment, and that certificates meet the following requirements:
  - A User Principal Name (UPN) must correspond to an Active Directory account in the Subject Alternative Name (SAN) extension.
  - The certificate must specify Client Authentication in the Application Policy or Enhanced Key Usage field or the browser does not show the certificate.
- Add an Active Directory identity source to vCenter Single Sign-On.
- Assign the vCenter Server Administrator role to one or more users in the Active Directory identity source. Those users can then perform management tasks because they can authenticate and they have vCenter Server administrator privileges.
- Ensure that you have set up the reverse proxy and restarted the physical or virtual machine.

If smart card authentication is enabled and other authentication methods are disabled, users are then required to log in using smart card authentication.

If user name and password authentication are disabled, and if problems occur with smart card authentication, users cannot log in. In that case, a root or administrator user can turn on user name and password authentication from the vCenter Server command line. The following command enables user name and password authentication.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

1. Obtain the certificates and copy them to a folder that the `sso-config` utility can see.
   a) Log in to the vCenter Server console, either directly or by using SSH.
   b) Enable the shell, as follows.

      ```
      shell
      chsh -s "/bin/bash" root
      csh -s "bin/appliance/sh" root
      ```

   c) Use WinSCP or a similar utility to copy the certificates to the `/usr/lib/vmware-sso/vmware-sts/conf` directory on the vCenter Server.
   d) Optionally disable the appliance shell, as follows.

      ```
      chsh -s "/bin/appliancesh" root
      ```

2. Log in with the vSphere Client to the vCenter Server.
3. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

4. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
5. Under the **Identity Provider** tab, click **Smart Card Authentication**, then click **Edit**.
6. Select or deselect authentication methods, and click **Save**.

   You can choose smart card authentication by itself, or both smart card authentication and password and Windows session authentication.

   You cannot enable or disable RSA SecurID authentication from this Web interface. However, if RSA SecurID has been enabled from the command line, the status appears in the Web interface.

   The **Trusted CA certificates** appears.
7. Under the **Trusted CA certificates** tab:
   a) Click **Add**, and click **Browse**.
   b) Select a trusted CA certificate, and click **Add**.
8. To add additional trusted CA certificates, repeat step 7.

Your environment might require enhanced OCSP configuration.

- If your OCSP response is issued by a different CA than the signing CA of the smart card, provide the OCSP signing CA certificate.
- You can configure one or more local OCSP responders for each vCenter Server site in a multi-site deployment. You can configure these alternative OCSP responders using the CLI. See Use the Command Line to Manage Smart Card Authentication.

Use the Command Line to Manage Smart Card Authentication

You can use the `sso-config` utility to manage smart card authentication from the command line. The utility supports all smart card configuration tasks.

- Verify that an enterprise Public Key Infrastructure (PKI) is set up in your environment, and that certificates meet the following requirements:
  - A User Principal Name (UPN) must correspond to an Active Directory account in the Subject Alternative Name (SAN) extension.
  - The certificate must specify Client Authentication in the Application Policy or Enhanced Key Usage field or the browser does not show the certificate.
- Add an Active Directory identity source to vCenter Single Sign-On.
- Assign the vCenter Server Administrator role to one or more users in the Active Directory identity source. Those users can then perform management tasks because they can authenticate and they have vCenter Server administrator privileges.
- Ensure that you have set up the reverse proxy and restarted the physical or virtual machine.

You can find the `sso-config` script at the following location:

```
/opt/vmware/bin/sso-config.sh
```

Configuration of supported authentication types and revocation settings is stored in VMware Directory Service and replicated across all vCenter Server instances in a vCenter Single Sign-On domain.

If user name and password authentication are disabled, and if problems occur with smart card authentication, users cannot log in. In that case, a root or administrator user can turn on user name and password authentication from the vCenter Server command line. The following command enables user name and password authentication.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

If you use the default tenant, use vsphere.local as the tenant name.

If you use OCSP for revocation check, you can rely on the default OCSP specified in the smart card certificate AIA extension. You can also override the default and configure one or more alternative OCSP responders. For example, you can set up OCSP responders that are local to the vCenter Single Sign-On site to process the revocation check request.

Note: If your certificate does not have OCSP defined, enable CRL (certificate revocation list) instead.

1. Obtain the certificates and copy them to a folder that the `sso-config` utility can see.
   a) Log in to the appliance console, either directly or by using SSH.
   b) Enable the appliance shell, as follows.

      ```
      shell
      chsh -s "/bin/bash" root
      ```

   c) Use WinSCP or a similar utility to copy the certificates to the `/usr/lib/vmware-sso/vmware-sts/conf` on the vCenter Server.
   d) Optionally disable the shell, as follows.

      ```
      chsh -s "/bin/appliancesh" root
      ```

2. To enable smart cart authentication, run the following command.

   ```
   sso-config.sh -set_authn_policy -certAuthn true -cacerts first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
   ```

   For example:

   ```
   sso-config.sh -set_authn_policy -certAuthn true -cacerts MySmartCA1.cer,MySmartCA2.cer  -t vsphere.local
   ```

   Separate multiple certificates with commas, but do not put spaces after the comma.

3. To disable all other authentication methods, run the following commands.

   ```
   sso-config.sh -set_authn_policy -pwdAuthn false -t vsphere.local
   sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
   sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
   ```

4. Optional: To set a certificate policies allowlist, run the following command.

   ```
   sso-config.sh -set_authn_policy -certPolicies policies
   ```

   To specify multiple policies, separate them with a comma, for example:

   ```
   sso-config.sh -set_authn_policy -certPolicies 2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
   ```

   This allowlist specifies object IDs of policies that are allowed in the certificate's certificate policy extension. An X509 certificate can have a Certificate Policy extension.

5. Optional: Turn on and configure revocation checking using OCSP.
   a) Turn on revocation checking using OCSP.

      ```
      sso-config.sh  -set_authn_policy -t tenantName  -useOcsp true
      ```

   b) If the OCSP responder link is not provided by the AIA extension of the certificates, provide the overriding OCSP responder URL and OCSP authority certificate.

      The alternative OCSP is configured for each vCenter Single Sign-On site. You can specify more than one alternative OCSP responder for your vCenter Single Sign-On site to allow for failover.

      ```
      sso-config.sh -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl http://ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
      ```

      Note: The configuration is applied to the current vCenter Single Sign-On site by default. Specify the `siteID` parameter only if you configure alternative OCSP for other vCenter Single Sign-On sites.

      Consider the following example.

      ```
       .sso-config.sh -t vsphere.local -add_alt_ocsp -ocspUrl http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
        Adding alternative OCSP responder for tenant :vsphere.local
      ```

```
OCSP responder is added successfully!
[
site::   78564172-2508-4b3a-b903-23de29a2c342
    [
    OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
    OCSP signing CA cert:   binary value]
    ]
    [
    OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
    OCSP signing CA cert:   binary value]
    ]
]
```

c) To display the current alternative OCSP responder settings, run this command.

```
sso-config.sh -t tenantName -get_alt_ocsp]
```

d) To remove the current alternative OCSP responder settings, run this command.

```
sso-config.sh -t tenantName -delete_alt_ocsp [-allSite] [-siteID pscSiteID_for_the_configuration]
```

6. Optional: To list configuration information, run the following command.

```
sso-config.sh -get_authn_policy -t tenantName
```

Set Revocation Policies for Smart Card Authentication

You can customize certificate revocation checking, and you can specify where vCenter Single Sign-On looks for information about revoked certificates.

- Verify that an enterprise Public Key Infrastructure (PKI) is set up in your environment, and that certificates meet the following requirements:
  - A User Principal Name (UPN) must correspond to an Active Directory account in the Subject Alternative Name (SAN) extension.
  - The certificate must specify Client Authentication in the Application Policy or Enhanced Key Usage field or the browser does not show the certificate.
- Verify that the vCenter Server certificate is trusted by the end user's workstation. Otherwise, the browser does not attempt authentication.
- Add an Active Directory identity source to vCenter Single Sign-On.
- Assign the vCenter Server Administrator role to one or more users in the Active Directory identity source. Those users can then perform management tasks because they can authenticate and they have vCenter Server administrator privileges.

You can customize the behavior by using the vSphere Client or by using the `sso-config` script. The settings that you select depend in part on what the CA supports.

- If revocation checking is disabled, vCenter Single Sign-On ignores any CRL or OCSP settings. vCenter Single Sign-On does not perform checks on any certificates.
- If revocation checking is enabled, the setup depends on the PKI setup.

OCSP only	If the issuing CA supports an OCSP responder, enable **OCSP** and disable **CRL as failover for OCSP**.
CRL only	If the issuing CA does not support OSCP, enable **CRL checking** and disable **OSCP checking**.
Both OSCP and CRL	If the issuing CA supports both an OCSP responder and a CRL, vCenter Single Sign-On checks the OCSP responder first. If the responder returns an unknown status or is not available, vCenter Single Sign-On checks the CRL. For this case, enable

both **OCSP checking** and **CRL checking**, and enable **CRL as failover for OCSP**.

- If revocation checking is enabled, advanced users can specify the following additional settings.

OSCP URL	By default, vCenter Single Sign-On checks the location of the OCSP responder that is defined in the certificate being validated. If the Authority Information Access extension is absent from the certificate or if you want to override it, you can explicitly specify a location.
Use CRL from certificate	By default, vCenter Single Sign-On checks the location of the CRL that is defined in the certificate being validated. Disable this option if the CRL Distribution Point extension is absent from the certificate or if you want to override the default.
CRL location	Use this property if you disable **Use CRL from certificate** and you want to specify a location (file or HTTP URL) where the CRL is located.

You can further limit which certificates vCenter Single Sign-On accepts by adding a certificate policy.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*`mydomain`*.
3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Under the **Identity Provider** tab, click **Smart Card Authentication**.
5. Click **Certificate revocation** and click **Edit** to enable or disable revocation checking.
6. If certificate policies are in effect in your environment, you can add a policy in the **Certificate policies** pane.

Set Up RSA SecurID Authentication

You can set up your environment to require that users log in with an RSA SecurID token. SecurID setup is supported only from the command line.

- Verify that your environment has a correctly configured RSA Authentication Manager and that users have RSA tokens. RSA Authentication Manager version 8.0 or later is required.
- Verify that the identity source that RSA Manager uses has been added to vCenter Single Sign-On. See Add or Edit a vCenter Single Sign-On Identity Source.
- Verify that the RSA Authentication Manager system can resolve the vCenter Server host name, and that the vCenter Server system can resolve the RSA Authentication Manager host name.
- Export the `sdconf.rec` file from the RSA Manager by selecting **Access** > **Authentication Agents** > **Generate configuration file**. To find `sdconf.rec` file, decompress the resulting `AM_Config.zip` file.
- Copy the `sdconf.rec` file to the vCenter Server node.

See the two vSphere Blog posts about RSA SecurID setup for details.

Note: RSA Authentication Manager requires that the user ID is a unique identifier that uses 1 to 255 ASCII characters. The characters ampersand (&), percent (%), greater than (>), less than (<), and single quote (`) are not allowed.

1. Change to the directory where the `sso-config` script is located.

   ```
   /opt/vmware/bin
   ```

2. To enable RSA SecurID authentication, run the following command.

   ```
   sso-config.sh -t tenantName -set_authn_policy -securIDAuthn true
   ```

   tenantName is the name of the vCenter Single Sign-On domain, vsphere.local by default.

3. Optional: To disable other authentication methods, run the following command.

   ```
   sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t vsphere.local
   ```

4. To configure the environment so that the tenant at the current site uses the RSA site, run the following command.

   ```
   sso-config.sh -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-sdConfFile Path]
   ```

   For example:

   ```
   sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
   ```

   You can specify the following options.

Option	Description
siteID	Optional Platform Services Controller site ID. Platform Services Controller supports one RSA Authentication Manager instance or cluster per site. If you do not explicitly specify this option, the RSA configuration is for the current Platform Services Controller site. Use this option only if you are adding a different site.
agentName	Defined in RSA Authentication Manager.
sdConfFile	Copy of the `sdconf.rec` file that was downloaded from RSA Manager and includes configuration information for the RSA Manager, such as the IP address.

5. Optional: To change the tenant configuration to nondefault values, run the following command.

   ```
   sso-config.sh -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size] [-maxLogFileCount-
    Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList Alg1,Alg2,...]
   ```

   The default is usually appropriate, for example:

   ```
   sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
   ```

6. Optional: If your identity source is not using the User Principal Name as the user ID, set up the identity source userID attribute. (Supported with Active Directory over LDAP identity sources only.)

   The userID attribute determines which LDAP attribute is used as the RSA userID.

   ```
   sso-config.sh -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr AttrName] [-siteID Loca-
   tion]
   ```

   For example:

   ```
   sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr userPrincipalName
   ```

7. To display the current settings, run the following command.

   ```
   sso-config.sh -t tenantName -get_rsa_config
   ```

If user name and password authentication is disabled and RSA authentication is enabled, users must log in with their user name and RSA token. User name and password login is no longer possible.

Note: Use the user name format *userID@domainName* or *userID@domain_upn_suffix*.

Managing the Login Message to the vSphere Client Login Page

You can create a message that is displayed on the vSphere Client login page.

You can set a message, disclaimer, or terms and conditions. Also, you can configure the message to require acknowledgment of the message before login.

Manage the Login Message to the vSphere Client Login Page

You can add a login message to the vSphere Client login page. You can also configure a custom login message and provide a check box for user consent.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Click the **Login Message** tab.
5. Click **Edit** and configure the login message.

Option	Description
Show login message	Toggle on **Show login message** to enable the login message. You cannot make changes to the login message unless you toggle on this switch.
Login message	Title of the message. By default, when **Consent checkbox** is toggled on, the login message text is `I agree to Terms and Conditions.` You must replace `Terms and Conditions` with your own text. If the **Consent checkbox** is toggled off, then `Login message` appears, over which you enter your message.
Consent checkbox	Toggle on **Consent checkbox** to require that the user clicks a check box before logging in. You can also display a message without a check box.
Details of login message	Message that the user sees when clicking the login message, for example, the text of the terms and conditions. You must enter some details in this text box.

6. Click **Save**.

vCenter Single Sign-On Security Best Practices

Follow vCenter Single Sign-On security best practices to protect your vSphere environment.

The vSphere authentication infrastructure enhances security in your vSphere environment. To make sure that infrastructure is not compromised, follow vCenter Single Sign-On best practices.

Check password expiration

The default vCenter Single Sign-On password policy has a password lifetime of 90 days. After 90 days, the password expires and you can no longer log in. Check the expiration and refresh passwords in a timely fashion.

Configure NTP

Ensure that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC). Synchronized systems are essential for vCenter Single Sign-On certificate validity, and for the validity of other vSphere certificates.

NTP also makes it easier to track an intruder in log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.

Troubleshooting Authentication

The following topics provide a starting point for troubleshooting vCenter Server authentication problems. Search this documentation center and the VMware Knowledge Base system for additional pointers.

Determining the Cause of a Lookup Service Error

vCenter Single Sign-On installation displays an error referring to the vCenter Server or the vSphere Client.

vCenter Server and Web Client installers show the error `Could not contact Lookup Service. Please check VM_ssoreg.log....`

This problem has several causes, including unsynchronized clocks on the host machines, firewall blocking, and services that must be started.

1. Verify that the clocks on the host machines running vCenter Single Sign-On, vCenter Server, and the Web Client are synchronized.
2. View the specific log file found in the error message.

   In the message, system temporary folder refers to `%TEMP%`.
3. Within the log file, search for the following messages.

   The log file contains output from all installation attempts. Locate the last message that shows `Initializing registration provider...`

Message	Cause and solution
`java.net.ConnectException: Connection timed out: connect`	The IP address is incorrect, a firewall is blocking access to vCenter Single Sign-On, or vCenter Single Sign-On is overloaded. Ensure that a firewall is not blocking the vCenter Single Sign-On port (by default 7444). Ensure also that the machine on which vCenter Single Sign-On is installed has adequate free CPU, I/O, and RAM capacity.
`java.net.ConnectException: Connection refused: connect`	The IP address or FQDN is incorrect and the vCenter Single Sign-On service has not started or has started within the past minute. Verify that vCenter Single Sign-On is working by checking the status of vCenter Single Sign-On vmware-sso daemon. Restart the service. If restarting does not correct the problem, see the recovery section of the *vSphere Troubleshooting Guide*.
`Unexpected status code: 404. SSO Server failed during initialization`	Restart vCenter Single Sign-On. If restarting does not correct the problem, see the Recovery section of the *vSphere Troubleshooting Guide*.
The error shown in the UI begins with `Could not connect to vCenter Single Sign-On`	You also see the return code `SslHandshakeFailed`. This error indicates that the provided IP address or FQDN that resolves to vCenter Single Sign-On host was not the address used when you installed vCenter Single Sign-On. In the `VM_ssoreg.log`, find the line that contains the following message. `host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>` where A was the FQDN you entered during the vCenter Single Sign-On installation, and B and C are system-generated allowable alternatives.

Message	Cause and solution
	Correct the configuration to use the FQDN on the right of the != sign in the log file. In most cases, use the FQDN that you specified during vCenter Single Sign-On installation. If none of the alternatives are possible in your network configuration, recover your vCenter Single Sign-On SSL configuration.

Unable to Log In Using Active Directory Domain Authentication

You log in to a vCenter Server component from the vSphere Client. You use your Active Directory user name and password. Authentication fails.

You add an Active Directory identity source to vCenter Single Sign-On, but users cannot log in to vCenter Server.

Users use their user name and password to log in to the default domain. For all other domains, users must include the domain name (user@domain or DOMAIN\user).

For all vCenter Single Sign-On deployments, you can change the default identity source. After that change, users can log in to the default identity source with user name and password only.

To configure your Integrated Windows Authentication identity source with a child domain within your Active Directory forest, see the VMware knowledge base article at http://kb.vmware.com/kb/2070433. By default, Integrated Windows Authentication uses the root domain of your Active Directory forest.

If changing the default identity source does not resolve the issue, perform the following additional troubleshooting steps.

1. Synchronize the clocks between the vCenter Server and the Active Directory domain controllers.
2. Verify that each domain controller has a pointer record (PTR) in the Active Directory domain DNS service.
   Verify that the PTR record information for the domain controller matches the DNS name of the controller. When using the vCenter Server, run the following commands to perform the task:
   1. To list the domain controllers, run the following command:
      ```
      # dig SRV _ldap._tcp.my-ad.com
      ```
      The relevant addresses are in the answer section, as in the following example:
      ```
      ;; ANSWER SECTION:
      _ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
      ...
      ```
   2. For each domain controller, verify forward and reverse resolution by running the following command:
      ```
      # dig my-controller.my-ad.com
      ```
      The relevant addresses are in the answer section, as in the following example:
      ```
      ;; ANSWER SECTION:
      my-controller.my-ad.com (...) IN A controller IP address
      ...
      # dig -x <controller IP address>
      ```
      The relevant addresses are in the answer section, as in the following example:
      ```
      ;; ANSWER SECTION:
      IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
      ...
      ```
3. If that does not resolve the problem, remove the vCenter Server from the Active Directory domain and then rejoin the domain. See the *vCenter Server Configuration* documentation.
4. Close all browser sessions connected to the vCenter Server and restart all services.
   ```
   /bin/service-control --restart --all
   ```

vCenter Server Login Fails Because the User Account Is Locked

When you log in to vCenter Server from the vSphere Client login page, an error indicates that the account is locked.

After several failed attempts, you cannot log in to the vSphere Client using vCenter Single Sign-On. You see the message that your account is locked.

You exceeded the maximum number of failed login attempts.

- If you attempted log in as a user from the system domain (vsphere.local by default), ask your vCenter Single Sign-On administrator to unlock your account. If the lock is set to expire in the lockout policy, you can wait until your account is unlocked. vCenter Single Sign-On administrators can use CLI commands to unlock your account.
- If you log in as a user from an Active Directory or LDAP domain, ask your Active Directory or LDAP administrator to unlock your account.

VMware Directory Service Replication Can Take a Long Time

If your environment includes multiple vCenter Server instances connected through enhanced linked mode, and if one of the vCenter Server instances becomes unavailable, your environment continues to function. When the vCenter Server becomes available again, user data and other information are usually replicated within 30 seconds with partners connected through enhanced linked mode. In certain circumstances, however, replication might take a long time.

In certain situations, for example, when your environment includes multiple vCenter Server instances in different locations, and you make significant changes while one vCenter Server is unavailable, you do not see replication across VMware Directory Service instances right away. For example, you do not see a new user that was added to the available vCenter Server instance in the other instance until replication is complete. Replication might take a long time, depending on your enhanced linked mode topology.

During normal operation, changes to a VMware Directory Service (vmdir) instance in one vCenter Server instance (node) show up in its direct replication partner within about 30 seconds. Depending on the replication topology, changes in one node might have to propagate through intermediate nodes before they arrive at each vmdir instance in each node. Information that is replicated includes user information, certificate information, license information for virtual machines that are created, cloned, or migrated with VMware vMotion, and more.

When the replication link is broken, for example, because of a network outage or because a node becomes unavailable, changes in the federation do not converge. After the unavailable node is restored, each node tries to catch up with all changes. Eventually, all vmdir instances converge to a consistent state but it might take a while to reach that consistent state if many changes occurred while one node was unavailable.

Your environment functions normally while replication happens. Do not attempt to solve the problem unless it persists for over an hour.

Export a vCenter Server Support Bundle

You can export a support bundle that contains the log files for the vCenter Server services from the vSphere Client, or by using an API. After the export, you can explore the logs locally or send the bundle to VMware Support.

Verify that the vCenter Server is successfully deployed and running.

For more information about the API, see *vCenter Server Management Programming Guide*.

1. From a Web browser, connect to the vCenter Server configuration management interface at https://*vcenter_server_ip*:5480.
2. Log in as the root user for the vCenter Server.
3. From the **Actions** menu, select **Create Support Bundle**.
4. Unless browser settings prevent an immediate download, the support bundle is saved to your local machine.

Authentication Services Logs Reference

The vCenter Server authentication services use syslog for logging. You can examine the log files to determine the reasons for failures.

Table 114: Service Logs

Service	Description
VMware Directory Service	By default, vmdir logging goes to `/var/log/messages` or `/var/log/vmware/vmdird/`. For issues at deployment time, `/var/log/vmware/vmdir/vmafdvmdirclient.log` might also contain useful troubleshooting data.
VMware Single Sign-On	vCenter Single Sign-On logging goes to `/var/log/vmware/sso/`.
VMWare Certificate Authority (VMCA)	VMCA service log is located in `/var/log/vmware/vmcad/vmcad-syslog.log`.
VMware Endpoint Certificate Store (VECS)	VECS service log is located in `/var/log/vmware/vmafdd/vmafdd-syslog.log`.
VMware Lookup Service	Lookup service log is located in `/var/log/vmware/sso/lookupServer.log`.

Managing Host and Cluster Lifecycle

Managing Host and Cluster Lifecycle provides information about configuring and using VMware®vSphere Lifecycle Manager to manage the ESXi hosts and clusters in your environment.

Managing Host and Cluster Lifecycle provides instructions for configuring vSphere Lifecycle Manager, working with the vSphere Lifecycle Manager depot, and using baselines and images to install, update, or upgrade the software and firmware running on your ESXi hosts.

Managing Host and Cluster Lifecycle also provides detailed guidelines about using vSphere Lifecycle Manager recommended images and performing hardware compatibility checks on single hosts or clusters. It also describes how you can configure and use the Update Manager Download Service (UMDS) to download software updates in deployments with no access to the Internet.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

This information is intended for experienced system administrators who are familiar with data center operations and virtual machine technology.

Client Interface

The instructions in this guide reflect the HTML5-based vSphere Client.

Updated Information

This *Managing Host and Cluster Lifecycle* is updated with each release of the product or when necessary.

This table provides the update history of the *Managing Host and Cluster Lifecycle*.

Revision	Description
24 MAR 2025	• Added information about the changes to the online depot URLs in Online and Offline Depots, Configuring the Download Sources, and Installing, Setting Up, and Using Download Service.
14 MAR 2023	• Updated the requirements for using vSphere Lifecycle Manager images for Supervisor Clusters in vSphere Lifecycle Manager and vSphere with Tanzu with vSphere Networking and vSphere Lifecycle Manager and vSphere with Tanzu with NSX-T Data Center Networking . • Added information about the Cisco hardware support manager integration in Deploying Hardware Support Managers.
24 NOV 2022	• Added the privilege needed as a prerequisite in the Automatically Upgrade VMware Tools on Reboot procedure. • Provided a link to the VMware Compatibility Guide in Deploying Hardware Support Managers.
23 JUN 2022	Added RHEL 8.5, RHEL 8.6, and RHEL 9.0 to the list of supported Linux systems for using UMDS. See Supported Linux-Based Operating Systems for Installing UMDS.

Revision	Description
11 APR 2022	• Added information about secure hash algorithms and the signature checks that vSphere Lifecycle Manager performs, see Secure Hashing and Signature Verification in vSphere Lifecycle Manager . • Added information about vSAN-generated recommendations and health alarms for vSAN clusters that you manage with vSphere Lifecycle Manager images, see Managing a vSAN Cluster with a Single Image.
05 OCT 2021	Initial release.

About vSphere Lifecycle Manager

VMware vSphere®vSphere Lifecycle Manager enables centralized and simplified lifecycle management for VMware ESXi hosts through the use of images and baselines.

What Is Lifecycle Management?

Lifecycle management refers to the process of installing software, maintaining it through updates and upgrades, and decommissioning it.

In the context of maintaining a vSphere environment, your clusters and hosts in particular, lifecycle management refers to tasks such as installing ESXi and firmware on new hosts, and updating or upgrading the ESXi version and firmware when required.

vSphere Lifecycle Manager General Overview

vSphere Lifecycle Manager is a service that runs in vCenter Server and uses the embedded vCenter Server PostgreSQL database. No additional installation is required to start using that feature. Upon deploying the vCenter Server appliance, the vSphere Lifecycle Manager user interface becomes automatically enabled in the HTML5-based vSphere Client.

vSphere Lifecycle Manager encompasses the functionality that Update Manager provides in earlier vSphere releases and enhances it by adding new features and options for ESXi lifecycle management at a cluster level.

In vSphere releases earlier than 7.0, Update Manager provides you with the ability to use baselines and baseline groups for host patching and host upgrade operations. Starting with vSphere 7.0, vSphere Lifecycle Manager introduces the option of using vSphere Lifecycle Manager images as an alternative way to manage the lifecycle of the hosts and clusters in your environment. You can also use vSphere Lifecycle Manager to upgrade the virtual machine hardware and VMware Tools versions of the virtual machines in your environment.

vSphere Lifecycle Manager can work in an environment that has access to the Internet, directly or through a proxy server. It can also work in a secured network without access to the Internet. In such cases, you use the Update Manager Download Service (UMDS) to download updates to the vSphere Lifecycle Manager depot, or you import them manually.

vSphere Lifecycle Manager Operations

The basic vSphere Lifecycle Manager operations are related to maintaining an environment that is up-to-date and ensuring smooth and successful updates and upgrades of the ESXi hosts.

Operation	Description
Compliance Check	An operation of scanning ESXi hosts to determine their level of compliance with a baseline attached to the cluster or with the image that the cluster uses. The compliance check does not alter the object.

Operation	Description
Remediation Pre-Check	An operation that you perform before remediation to ensure that the health of a cluster is good and that no issues occur during the remediation process.
Remediation	An operation of applying software updates to the ESXi hosts in a cluster. During remediation, you install software on the hosts. Remediation makes a non-compliant host compliant with the baselines attached to the cluster or with the image for cluster.
Staging	An operation that is available only for clusters that you manage with baselines or baseline groups. When you stage patches or extensions to an ESXi host, you download patch and extension VIBs to the host without applying them immediately. Staging makes the patches and extensions available locally on the hosts.

The vSphere Lifecycle Manager Depot

Several components make up vSphere Lifecycle Manager and work together to deliver the vSphere Lifecycle Manager functionality and coordinate the major lifecycle management operations that it provides for. The vSphere Lifecycle Manager depot is an important component in the vSphere Lifecycle Manager architecture, because it contains all software updates that you use to create vSphere Lifecycle Manager baselines and images. You can use vSphere Lifecycle Manager only if the vSphere Lifecycle Manager depot is populated with components, add-ons, base images, and legacy bulletins and patches.

For more information about software updates, see Bulletins, Components, Add-Ons, and ESXi Base Images.

For more information about the vSphere Lifecycle Manager depot, see Working with the vSphere Lifecycle Manager Depot.

Secure Hashing and Signature Verification in vSphere Lifecycle Manager

vCenter Server performs an automatic hash check on all software that vSphere Lifecycle Manager downloads from online depots or from a UMDS-created depot. Similarly, vCenter Server performs an automatic checksum check on all software that you manually import into the vSphere Lifecycle Manager depot. The hash check verifies the sha-256 checksum of the downloaded software to ensure its integrity. During remediation, before vSphere Lifecycle Manager installs any software on a host, the ESXi host checks the signature of the installable units to verify that they are not corrupted or altered during the download.

When you import an ISO image into the vSphere Lifecycle Manager depot, vCenter Server performs an MD5 hash check on the ISO image to validate its MD5 checksum. During remediation, before the ISO image is installed, the ESXi host verifies the signature inside the image.

If an ESXi host is configured with UEFI Secure Boot, the ESXi host performs full signature verification of each package that is installed on the host every time the host boots. For more information, see the *vSphere Security* documentation.

vSphere Lifecycle Manager Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

The vSphere Lifecycle Manager User Interface in the vSphere Client

After you deploy the vCenter Server appliance, vSphere Lifecycle Manager becomes immediately visible in the vSphere Client.

The vSphere Lifecycle Manager user interface has two main views, which for convenience this guide calls the home view and the compliance view.

vSphere Lifecycle Manager Home View

The vSphere Lifecycle Manager home view is where you configure and administer the vSphere Lifecycle Manager instance that runs on your vCenter Server system. You go to the vSphere Lifecycle Manager home view to configure how vSphere Lifecycle Manager baselines and images work.

You do not need any special privilege to access the vSphere Lifecycle Manager home view.

To access the vSphere Lifecycle Manager home view in the vSphere Client, select **Menu** > **Lifecycle Manager**.

In the vSphere Lifecycle Manager home view, you specify the vSphere Lifecycle Manager instance that you want to administer by selecting a vCenter Server system from the drop-down menu at the top of the **Lifecycle Manager** pane.

In the **Lifecycle Manager** pane, you have the following top-level tabs: **Image Depot**, **Updates**, **Imported ISOs**, **Baselines**, and **Settings**.

You use the **Image Depot** tab when you work vSphere Lifecycle Manager images. You use the **Updates**, **Imported ISOs**, and **Baselines** tabs when you work with vSphere Lifecycle Manager baselines. For more information about the **Image Depot**, **Updates**, and **Imported ISOs** tabs, see Browsing the vSphere Lifecycle Manager Depot.

The **Settings** tab is where you configure all vSphere Lifecycle Manager remediation settings and download sources. You use the **Settings** with both vSphere Lifecycle Manager images and baselines. For more information about configure the vSphere Lifecycle Manager settings, see Configuring the vSphere Lifecycle Manager Remediation Settings.

In the vSphere Lifecycle Manager home view, you can perform the following tasks:

- Browse the vSphere Lifecycle Manager depot.
- Trigger the synchronization of updates with the configured online depots.
- Trigger the synchronization of hardware compatibility data.
- Import offline depots manually.
- Import ISO images to use for the creation of upgrade baselines.
- Create and manage baselines and baseline groups.
- Configure the default vSphere Lifecycle Manager download source.
- Add a URL to an online depot to the list of download sources.
- Allow or disallow downloading from a download source.
- Configure host remediation settings.
- Configure virtual machine rollback settings.

vSphere Lifecycle Manager Compliance View

The vSphere Lifecycle Manager compliance view is where you perform the major vSphere Lifecycle Manager operations - checking the compliance of ESXi hosts against a baseline or an image, staging, remediation pre-checks, remediation, and so on.

You go to the vSphere Lifecycle Manager compliance view to actually use the vSphere Lifecycle Manager baselines and images on your clusters and hosts.

To access the vSphere Lifecycle Manager compliance view in the vSphere Client, you must have the **View Compliance Status** privilege.

Generally, the vSphere Lifecycle Manager compliance view is on the **Updates** tab for a selected object.

Depending on the selected object and whether you use baselines or images to manage the object, you access the vSphere Lifecycle Manager compliance view in two different ways.

- To access the vSphere Lifecycle Manager compliance view for a host or a cluster that you manage with baselines, go to the **Updates** tab for the object and select **Baselines**.
  In the **Baselines** pane of the vSphere Lifecycle Manager compliance view, you can perform the following tasks:
  – Check the compliance status of ESXi hosts and clusters against baselines or baseline groups.
  – Attach and detach baselines and baseline groups to hosts and clusters.
  – Generate a remediation pre-check report that lists recommended actions to ensure successful remediation.
  – Stage patches or extensions to hosts.
  – Check the compliance status of ESXi hosts against an image.
  – Remediate hosts against baselines and baseline groups.
  – Remediate hosts that are part of a vSAN cluster against system-managed baselines.
- To access the vSphere Lifecycle Manager compliance view for a cluster that you manage with a single image, go to the **Updates** tab for the cluster and select **Image**.
  In the **Image** pane of the vSphere Lifecycle Manager compliance view, you can perform the following tasks:
  – Export, import, and edit the image that the cluster uses.
  – Upgrade the firmware of the ESXi hosts in the cluster.
  – Check for and view recommended images for the cluster.
  – Check the hardware compatibility for a selected ESXi version against vSAN HCL .
  – Check the compliance status of the ESXi hosts against the image.
  – Run a remediation pre-check to ensure successful remediation.
  – Remediate the ESXi hosts against the image that the cluster uses.

On the the **Updates** tab, you can also perform other tasks.

- Under **Hosts**, select **Hardware Compatibility** to check the hardware compatibility of a host against the VMware Compatibility Guide.
- Under **Hosts**, select **VMware Tools** or **VM Hardware** to check the status of virtual machines and upgrade the VMware Tools version or the virtual hardware version of the virtual machines.

vSphere Lifecycle Manager and vCenter Server Single Sign-On Domain

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can configure the settings for each vSphere Lifecycle Manager instance. The modifications to the settings are applied only to the vSphere Lifecycle Manager instance that you specify and are not propagated to the other instances in the group. Similarly, you can use vSphere Lifecycle Manager to perform compliance and status checks, and remediate only those inventory objects that are managed by the vCenter Server system where the respective vSphere Lifecycle Manager instance runs.

Bulletins, Components, Add-Ons, and ESXi Base Images

To understand the difference between vSphere Lifecycle Manager images and vSphere Lifecycle Manager baselines, you must understand the relation between the basic software packaging types that software vendors use to create and ship software updates.

vSphere Lifecycle Manager uses software from VMware, OEMs, and third-party software providers.

- OEMs are VMware partners, for example, Dell, HPE, VMware Cloud on AWS.
- Third-party software providers are providers of I/O filters, device drivers, CIM modules, and so on.

vSphere Installation Bundles (VIBs)

The VIB is the basic building block for the creation of installation packages for ESXi hosts. A VIB is a software package that contains metadata and a binary payload, which represents the actual piece of software to be installed on ESXi. The

VIB does not represent an entire feature, but just a single module of the feature. So, the VIB is the smallest installable software unit that VMware and other software vendors ship.

Table 115: Related Terminology

Term	Definition
VIB Metadata	An XML file (`descriptor.xml`) that describes the contents of the VIB. It also contains dependency information, textual descriptions, system requirements, and information about bulletins.
Standalone VIB	A VIB that is not included in a bulletin or component.

vSphere Lifecycle Manager does not consume and work with individual VIBs. VIBs must be further packaged into a higher-level construct.

Bulletins

The bulletin is a grouping of one or more VIBs. Bulletins are defined within the metadata of the VIB. You use bulletins, and not individual VIBs, to create vSphere Lifecycle Manager baselines, which you attach to inventory objects and use to update and upgrade ESXi hosts.

Table 116: Related Terminology

Term	Definition
Patch	A small software update that provides bug fixes or enhancements to the current version of the software. A patch groups one or more VIBs together to address a particular issue or to provide enhancements to the current version of the software.
Roll-up Bulletin	A collection of patches that are grouped to facilitate downloads and deployment.
Extension	A bulletin that defines a group of VIBs for adding an optional component to an ESXi host. An extension is usually provided by a third party. The third-party provider is also responsible for providing patches and updates for the extension.

Components

Starting with vSphere 7.0, the component becomes the basic packaging construct for VIBs. VMware, OEMs, and third-party software providers now deliver software in the form of components. The component is a bulletin with additional metadata specifying the name and the version of the component. Unlike the bulletin, the component is a logical grouping of VIBs that provides you with a complete and visible feature upon installation.

VMware and OEMs do not deliver components independently. VMware bundles components together into fully functional and bootable ESXi base images. OEMs bundle components together into vendor add-ons. Third-party software vendors create and ship software, for example drivers or adapters, as independent components.

Base Images

The base image is an ESXi image that VMware provides with every release of ESXi. The base image is a collection of components that is complete and can boot up a server. Base images have a user-readable name and a unique version that is updated with every major or minor release of ESXi.

The version of a base image corresponds to an ESXi release and uses the following naming format:

- General Availability release: 7.0
- Update release: 7.0 U1, 7.0 U2
- Patch release: 7.0 a, 7.0 b
- Security patch release: 7.0 sa, 7.0 sb
- Patch after an update release: 7.0 U1 a, 7.0 U1 sa, 7.0 b, 7.0 sb

Base images are hosted and available in the VMware online depot. Additionally, you can download an ESXi installer ISO file and an offline bundle (ZIP file) that contains the ESXi version from my.vmware.com.

Vendor Add-Ons

OEMs pack one or multiple components into a unit called an add-on. You use vendor add-ons to customize an ESXi image with OEM content and drivers.

The add-on is a collection of components that does not represent a complete, bootable image. You cannot use vendor add-ons on their own. To customize an ESXi release, you must add the vendor add-on to an ESXi base image. The combination of a vendor add-on and an ESXi base image is practically identical to an OEM-provided custom image.

When combined with an ESXi base image, the add-on can add, update, or remove components that are part of the ESXi base image. In the vSphere Client, for each add-on available in the depot, you can view the list of components that it adds to an ESXi base image. Similarly, you can find information about the components that it removes from a base image.

Starting with vSphere 7.0, in addition to custom ISO images and offline bundles, OEMs can release ZIP files that contain only the vendor add-on, that is, the delta between the custom image and the ESXi base image. OEMs can release such add-on ZIP files at their discretion. The introduction of the concept of add-ons decouples the release cycle of OEMs from the release cycle of VMware. As a result, you can update vendor add-ons independently of updating the ESXi version of your hosts. Also, the vendor add-on decouples the OEM customization from the VMware stock image. As a result, you can combine software components more freely.

Bulletins and Components in the vSphere Lifecycle Manager Depot

vSphere Lifecycle Manager can consume both bulletins and components.

If you use baselines and baseline groups to manage hosts and clusters, vSphere Lifecycle Manager reads and lists the software updates that are available in the vSphere Lifecycle Manager depot as bulletins. You can find the list of available bulletins on the **Updates** tab in the vSphere Lifecycle Manager home view.

If you use vSphere Lifecycle Manager images to manage hosts and clusters, you can only work with components and the related notions of add-ons and base images. You can find the list of the components, add-ons, and ESXi base images on the **Image Depot** tab in the vSphere Lifecycle Manager home view.

vSphere Lifecycle Manager Baselines and Images

vSphere Lifecycle Manager enables you to manage ESXi hosts and clusters with images or baselines. vSphere Lifecycle Manager baselines and vSphere Lifecycle Manager images are different in their essence, the way they work, and the features they support.

You use vSphere Lifecycle Manager baselines and baseline groups to perform the following tasks.

- Upgrade and patch ESXi hosts.
- Install and update third-party software on ESXi hosts.

You use vSphere Lifecycle Manager images to perform the following tasks.

- Install a desired ESXi version on all hosts in a cluster.

- Install and update third-party software on all ESXi hosts in a cluster.
- Update and upgrade the ESXi version on all hosts in a cluster.
- Update the firmware of all ESXi hosts in a cluster.
- Generate recommendations and use a recommended image for your cluster.
- Check the hardware compatibility of hosts and clusters against the VMware Compatibility Guideand the vSAN Hardware Compatibility List.

vSphere Lifecycle Manager Images

You use vSphere Lifecycle Manager images to apply software and firmware updates to the ESXi hosts in a cluster. Using a single image to manage all hosts in a cluster ensures cluster-wide host image homogeneity.

You can use various methods and tools to deploy ESXi hosts and maintain their software lifecycle. For example, you can upgrade hosts by using VMware vSphere®ESXi™ Image Builder CLI, esxcli, vSphere Auto Deploy. The different deployment and upgrade choices involve different workflows and require you to use different ESXi image formats. When you use vSphere Lifecycle Manager images, you follow one workflow and use the same ESXi image format for all software lifecycle-related operations: install, upgrade, update, and patching, which significantly simplifies the lifecycle management process.

Understanding vSphere Lifecycle Manager Images

A vSphere Lifecycle Manager image represents a desired software specification to be applied to all hosts in a cluster. When you set up a vSphere Lifecycle Manager image, you can define the full software stack that you want to run on the hosts in a cluster: the ESXi version, additional VMware software, vendor and third-party software, for example firmware and drivers.

A vSphere Lifecycle Manager image can consist of the following four elements:

- ESXi base image
  The base image contains an image of VMware ESXi Server and additional components, such as drivers and adapters that are necessary to boot a server. The base image is the only mandatory element in a vSphere Lifecycle Manager image. All other elements are optional.
- Vendor add-on
  The vendor add-on is a collection of software components that OEMs create and distribute. The vendor add-on can contain drivers, patches, and solutions.
- Firmware and drivers add-on
  The firmware and drivers add-on is a special type of vendor add-on designed to assist in the firmware update process. The firmware and drivers add-on contains firmware for a specific server type and corresponding drivers. To add a firmware and drivers add-on to your image, you must install the hardware support manager plug-in provided by the hardware vendor for the hosts in the respective cluster.
- Independent components
  The component is the smallest discrete unit in an image. The independent components that you add to an image contain third-party software, for example drivers or adapters.

You can set up a vSphere Lifecycle Manager image for a cluster during the creation of the cluster. Alternatively, for existing clusters that you mange with vSphere Lifecycle Manager baselines, you can switch from using baselines to using images at a later time.

Note:

If you switch to using images, you cannot revert to using baselines for that cluster. You can only move the hosts to a cluster that uses baselines.

The Desired State Model

The concept of images that vSphere Lifecycle Manager introduces is based on the Desired State model for managing ESXi hosts and clusters.

The desired state of an ESXi host represents both the target software and target configuration for the host as opposed to the software and configuration that it currently runs. The Desired State model is the idea of managing hosts and clusters by defining and applying a desired state instead of listing and following steps to change the current state.

vSphere Lifecycle Manager Baselines and Baseline Groups

You use baselines and baseline groups to update and upgrade the ESXi hosts in your environment. To start managing a cluster with baselines and baseline groups, you must skip setting up an image during the creation of the cluster.

Baselines

A baseline is a grouping of multiple bulletins. You can attach a baseline to an ESXi host and check the compliance of the host against the associated baseline.

Baselines can be classified according to different criteria.

- Depending on the type of content, baselines are patch baselines, extension baselines, and upgrade baselines. Patch and extension baselines contain bulletins of the respective kind. Upgrade baselines contain ESXi images.
- Depending on how the update content is selected, baselines are fixed and dynamic.
- Depending on how they are created and managed, baselines are predefined, recommendation, or custom baselines.

Baseline Groups

A baseline group is a collection of non-conflicting baselines. You can attach the entire baseline group to an inventory object to check the compliance status of the object against all the baselines in the group as a whole.

You can combine custom baselines with any of the predefined baselines to create baseline groups.

Host baseline groups can contain a single upgrade baseline, and various patch and extension baselines.

To update or upgrade ESXi hosts by using baselines or baseline groups, you must first attach the baselines or baselines group to an inventory object.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and data centers. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

For more information about creating and managing baselines and baseline groups, see Creating and Working with Baselines and Baseline Groups.

Comparison Between vSphere Lifecycle Manager Images and Baselines

A vSphere Lifecycle Manager baseline is a collection of bulletins. A vSphere Lifecycle Manager image is a collection of components. Some differences exist between the operations that you can perform with a vSphere Lifecycle Manager image and the operations that you can perform with vSphere Lifecycle Manager baselines.

Operation	Baselines	Images
Distribution	Bulletins are distributed through online depots and as offline bundles. You can import and use ISO images to create upgrade baselines.	Base image, vendor add-ons, and components are distributed through online depots and as offline bundles. You cannot use ISO images to set up a vSphere Lifecycle Manager image for a cluster.
Validation	Not supported. You do not validate a baseline before applying the updates to the hosts. You can only perform a remediation pre-check.	Supported. You can validate a vSphere Lifecycle Manager image to check if it is applicable to all hosts in the cluster. You can also perform a remediation pre-check.
Import/Export	You can create a custom baseline and attach it to different objects in the same vCenter Server instance. You cannot export baselines and distribute them across vCenter Server instances.	You can export an image and use it to manage other clusters in the same or in a different vCenter Server instance. Images are portable across vCenter Server instances. You can export an image as an ISO or JSON file, but you can only import images that are in a JSON format.
Compliance checks	With baselines, you can check the compliance of an object against a single or against multiple baselines.	With vSphere Lifecycle Manager images, you can check the compliance of the hosts against a single image. To check the compliance against another image, you must first set up the new image.
Staging	You can stage updates to the hosts before actually installing them.	Not supported.
Remediation	With vSphere Lifecycle Manager baselines, you can remediate an object against a single baseline or against multiple baselines. So, with a single operation, you can patch and upgrade a host. However, vSphere Lifecycle Manager baselines list the updates to be applied to hosts, but the remediation result is not always predictable, because ESXi image on the hosts might change after remediation.	With vSphere Lifecycle Manager images, you can add, remove, or modify the components in the image that you use for a cluster. When you remediate the hosts against the new image, all modified components are applied to the host. So, you can upgrade and patch a host with a single remediation operation. vSphere Lifecycle Manager images define the precise image to be applied to the hosts after remediation. No deviation from the defined image is possible after remediation. vSphere Lifecycle Manager does not allow solutions to push VIBs to the hosts.
Firmware updates	Not supported.	With vSphere Lifecycle Manager images, firmware updates are carried out through firmware and drivers add-ons, which you add to the image that you use to manage a cluster. Updating firmware with images requires an OEM-provided hardware support manager plug-in, which integrates with vSphere Lifecycle Manager.
Hardware compatibility checks	Not supported.	You can check the hardware compatibility of the hosts in a cluster against the VMware Compatibility Guide (VCG). You can also check the compatibility of all hosts in a vSAN-enabled cluster against the vSAN Hardware Compatibility List (vSAN HCL).

Operation	Baselines	Images
Software recommendations	Limited support. Software recommendations are only available for vSAN clusters in the form of recommendation baselines.	Supported. Based on the hardware of the hosts in the cluster, you get recommendations about available and applicable ESXi updates or upgrades.
vCenter Server /Datacenter-level operations	With vSphere Lifecycle Manager baselines, you can trigger any of the main operations at the vCenter Server or data center level.	With vSphere Lifecycle Manager images, you cannot operate at a vSphere Lifecycle Manager or data center level.
Virtual machine management	You can upgrade the VMware Tools and virtual hardware versions of the virtual machines in a cluster that you manage with vSphere Lifecycle Manager baselines.	You can upgrade the VMware Tools and virtual hardware versions of the virtual machines in a cluster that you manage with vSphere Lifecycle Manager images.
Update Manager Download Service (UMDS)	Supported.	Supported.
Remote Office/Branch Office (ROBO) support	Not provided. Although no specific optimization exists for ROBO deployments, you can still use baselines and baseline groups with ROBO clusters.	Provided. With vSphere Lifecycle Manager images, you can set up a local depot and use it in ROBO environments. For more information, see Manage Depot Overrides for a Cluster.
REST APIs	Not available.	Available.

System Requirements for Using vSphere Lifecycle Manager

Depending on whether you want to use baselines or images for software lifecycle management, you must comply with a different set of requirements. To achieve your goals, you must also know the specifics in behavior and limitations that vSphere Lifecycle Manager has.

Table 117: System Requirements for Using vSphere Lifecycle Manager

Scenario	Requirements
Using a single image to manage a cluster.	• All ESXi hosts in the cluster must be of version 7.0 and later. • All ESXi hosts in the cluster must be stateful. A stateful install is one in which the host boots from a disk. • All ESXi hosts in the cluster must be from the same vendor and with identical hardware. Different generations and models of servers need different software drivers, which implies that you must set up different vSphere Lifecycle Manager images to manage each generation or model. However, with vSphere Lifecycle Manager, you use one single image for the entire cluster. Also, vSphere Lifecycle Manager does not detect and handle the hardware differences between the hosts in the cluster. You can use a vSphere Lifecycle Manager image to manage a heterogeneous cluster only if the vSphere Lifecycle Manager image for the cluster includes vendor customization, for example a vendor or firmware add-on, that can address and handle the hardware differences across the hosts in the cluster, which is a rare scenario.

Scenario	Requirements
	• The cluster must include only integrated solutions. For example: – VMware vSAN™ – VMware vSphere® High Availability (HA) – vSphere with Tanzu – NSX-T Data Center
Using baselines and baseline groups to manage a cluster.	• To use baselines for ESXi host patching operations, vSphere Lifecycle Manager works with ESXi 6.5, ESXi6.7, and ESXi7.0. • To use baselines for ESXi host upgrade operations, vSphere Lifecycle Manager works with ESXi 6.5, ESXi6.7, and their respective Update releases.
Switching from using baselines to using a single image to manage a cluster.	• The cluster must meet the requirements for using an image. • The cluster must be eligible for the transition. For more information about the **Check cluster's eligibility to be managed with a single image** task, see Cluster Eligibility to Use vSphere Lifecycle Manager Images.
Upgrading virtual machine hardware and VMware Tools	For VMware Tools and virtual machine hardware upgrade operations, vSphere Lifecycle Manager works with ESXi 6.5, ESXi6.7, and ESXi7.0.

Privileges for Using vSphere Lifecycle Manager Images and Baselines

To configure vSphere Lifecycle Manager settings and to use successfully vSphere Lifecycle Manager baselines and images, you must have the proper privileges.

You can assign vSphere Lifecycle Manager privileges to different roles from the vSphere Lifecycle Manager client interface in the vSphere Client.

vSphere Lifecycle Manager Privileges For Using Images

When you use vSphere Lifecycle Manager images, you need a different set of privileges for each task.

Table 118: VMware vSphere vSphere Lifecycle Manager Privileges For Using Images

Task	Required Privileges
Set Up Image	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Write** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read**
Import Image	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Write** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read** • **Upload File** > **Upload File**
Export Image	**VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read**

Task	Required Privileges
Edit Image	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Write** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read**
Work with Recommendations	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Write** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read**
Work with Depot	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Write**
Manage Depot Overrides	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Write**
Check Compliance	**VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read**
Run Remediation Pre-Check	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: General Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **ESXi Health Perspectives** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Remediation Privileges** > **Read**
Remediate Against an Image	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: General Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **ESXi Health Perspectives** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Remediation Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Remediation Privileges** > **Write** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read**
Edit Remediation Settings	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Write**
Update Firmware	• **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Read** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Image Privileges** > **Write** • **VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Settings Privileges** > **Read**
View Hardware Compatibility	**VMware vSphere Lifecycle Manager** > **Lifecycle Manager: Hardware Compatibility Privileges** > **Access Hardware Compatibility**

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

vSphere Lifecycle Manager Privileges For Using Baselines

Each of the vSphere Lifecycle Manager privileges that you need to use baselines and baseline groups covers a distinct functionality.

Table 119: VMware vSphere Lifecycle Manager Privileges For Using Baselines

Task	Privilege	Description
Configure	**Configure** > **Configure Service**	Configure the vSphere Lifecycle Manager service and the scheduled patch download task.
Manage Baseline	**Manage Baselines** > **Attach Baseline**	Attach baselines and baseline groups to objects in the vSphere inventory.
	Manage Baselines > **Manage Baselines**	Create, edit, or delete baselines and baseline groups.
Manage Patches and Upgrades	**Manage Patches and Upgrades** > **Remediate to Apply Patches, Extensions, and Upgrades**	Remediate virtual machines and hosts to apply patches, extensions, or upgrades. In addition, this privilege allows you to view the compliance status of objects.
	Manage Patches and Upgrades > **Scan for Applicable Patches, Extensions, and Upgrades**	Scan virtual machines and hosts to search for applicable patches, extensions, or upgrades.
	Manage Patches and Upgrades > **Stage Patches and Extensions**	Stage patches or extensions to hosts. In addition, this privilege allows you to view the compliance status of hosts.
	Manage Patches and Upgrades > **View Compliance Status**	View baseline compliance information for an object in the vSphere inventory.
Upload File	**Upload File** > **Upload File**	Upload upgrade images and offline patch bundles.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

Working with the vSphere Lifecycle Manager Depot

The vSphere Lifecycle Manager depot is the source of software updates for vSphere Lifecycle Manager. Conceptually, the vSphere Lifecycle Manager depot represents all software available for consumption to vSphere Lifecycle Manager.

The vSphere Lifecycle Manager depot is a local depot on the vCenter Server machine. It contains all the content from the online and offline depots that you use with vSphere Lifecycle Manager.

You can work with vSphere Lifecycle Manager only if the vSphere Lifecycle Manager depot contains software packages. For example, ESXi base images, vendor add-ons, third-party components, and legacy patches and updates. For more information about ESXi base images, vendor add-ons, components, and patches, see Bulletins, Components, Add-Ons, and ESXi Base Images.

You control how the vSphere Lifecycle Manager depot gets populated with software. You can configure vSphere Lifecycle Manager to download updates from online depots, or a UMDS-created shared repository. Alternatively, you can use offline depots to import updates into the vSphere Lifecycle Manager depot. For more information about the different types of depots that vSphere Lifecycle Manager can use, see vSphere Lifecycle Manager Download Sources.

Online and Offline Depots

vSphere Lifecycle Manager can consume software updates only if they are delivered in an online depot, as an offline depot, or as an installable ISO image. So, VMware, OEMs, and third-party software vendors must ship their software updates in any of these three formats.

Online Depots

An online depot is the hosted version of the software updates that VMware, OEMs, and third-party software providers ship. You access an online depot through a URL.svSphere Lifecycle Manager downloads to the vSphere Lifecycle Manager depot the content from the online depots that you configure it to use. vSphere Lifecycle Manager is preconfigured to download updates from the default VMware online depot. You can use the vSphere Client to access third-party online depots that contain additional components.

Synchronization is the process through which the contents of the online depots that you configure vSphere Lifecycle Manager to use get into the vSphere Lifecycle Manager depot. During synchronization, only the software metadata is downloaded. The actual payloads are downloaded when they are needed, for example during staging or remediation. When you deploy vCenter Server, vSphere Lifecycle Manager synchronizes with the official VMware online depot automatically. After the initial synchronization, you can schedule a download task to run at regular intervals or you can initiate a download task manually.

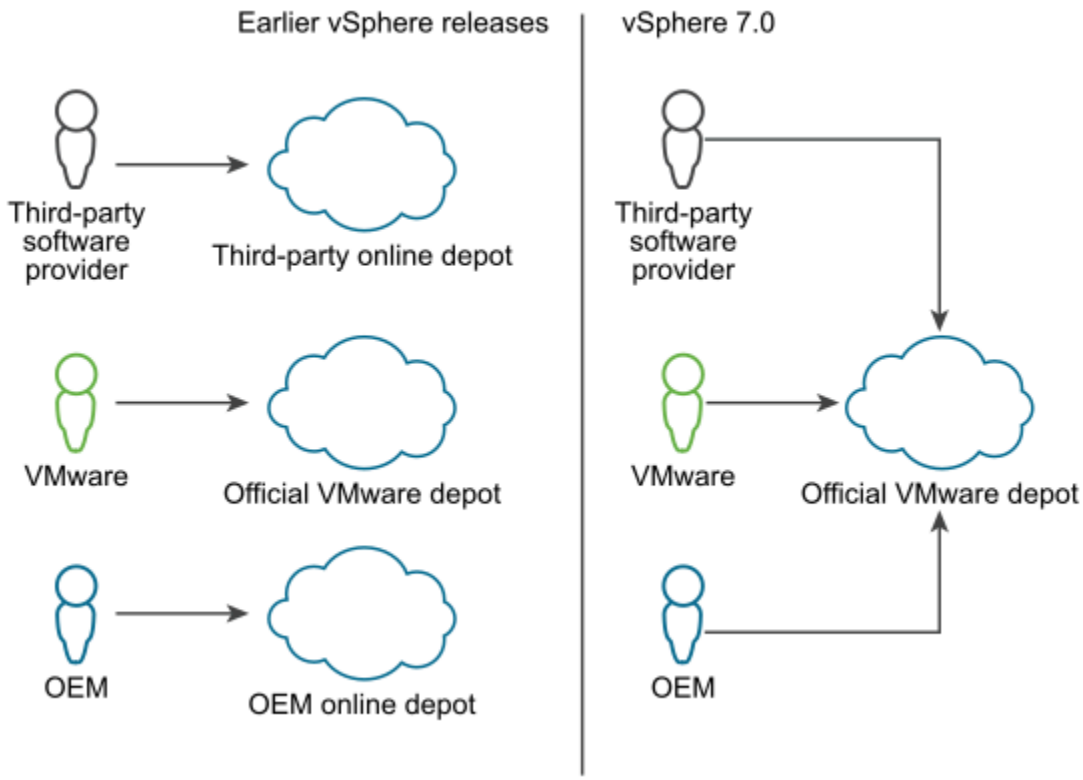
The Default VMware Online Depot

The default online depot that VMware provides hosts ESXi base images, vendor add-ons, ESXi-compatible I/O device drivers certified by VMware, and async VMware Tools releases. By default, vSphere Lifecycle Manager is configured to use the official VMware online depot as a download source for software updates.

Note:

The default online depot URLs are now unique for each customer. To update the default URLs of the online depot, see the following KB article: https://knowledge.broadcom.com/external/article/390121.

Unlike earlier vSphere releases, all software that you need to install, update, or customize the ESXi version of your hosts is available in the official VMware online depot.



Firmware updates are not hosted in the VMware depot. To perform firmware updates, you must install the hardware support manager plug-in that your hardware vendor provides. The plug-in gives you access to depots that contain the necessary firmware and related drivers updates.

In the vSphere Client, you can list additional online depots for vSphere Lifecycle Manager to download additional third-party components from, for example CIM modules. However, working with additional third-party depots and independent components is rarely necessary. In most cases, the vendor add-ons that are available in the official VMware depot provide full OEM customization for ESXi.

All software updates hosted in the official VMware online depot are also available as offline bundles, which you can download from the Broadcom Support Portal Downloads site and import manually to the vSphere Lifecycle Manager depot.

Offline Depots

An offline depot, also called an offline bundle, is a ZIP file that you download from the Internet or copy from a media drive and you save on a local or a shared network drive. You then can import the offline bundle to the vSphere Lifecycle Manager depot. You can also download offline bundles from the the Broadcom Support Portal Downloads website or from the websites of third-party vendors.

In addition to distributing an `offline.zip` file, or offline bundle, and a custom ISO image, OEMs distribute an `Add-on.zip` file that contains the delta between the OEM custom image and the base image that VMware provides. For more information about OEM add-ons, see Bulletins, Components, Add-Ons, and ESXi Base Images.

Import is the operation through which the contents of an offline bundle get into the vSphere Lifecycle Manager depot. During an import operation, both the software metadata and the actual payloads are downloaded into the vSphere Lifecycle Manager depot.

Table 120: Software Deliverables and Corresponding Distribution Formats

Software Vendor	Software Deliverable	Software Distribution Format
VMware	Base images	• The default VMware online depot • Offline bundle • ISO image
OEMs	Add-ons	• The default VMware online depot • Offline bundle • Add-on ZIP file • ISO image
Third-party software providers	Components	For device drivers that are certified by VMware: • The default VMware online depot • Offline bundle For other third-party software that is verified and certified by OEMs, for example I/O filters, CIM module: • An online depot • Offline bundle

vSphere Lifecycle Manager Download Sources

You can configure vSphere Lifecycle Manager to download software from the Internet or, in air-gap scenarios, from a UMDS-created shared repository.

Download Updates from the Internet

If you configure vSphere Lifecycle Manager to use the Internet, then the download sources are practically all online depots that you use for downloading software.

vSphere Lifecycle Manager is preconfigured to use the official VMware online depot. In the vSphere Client, you can list additional online depots for vSphere Lifecycle Manager to download additional third-party components from, for example CIM modules.

Note:

The URLs of the official VMware online depot are now unique for each customer. To update the download sources URLs, see the following KB articles: https://knowledge.broadcom.com/external/article/390121 and https://knowledge.broadcom.com/external/article/390123.

When vSphere Lifecycle Manager synchronizes to online depots, it downloads only the metadata of the updates. The actual payload is downloaded during staging or remediation.

Download Updates from a UMDS Depot

In vCenter Server deployments without access to the Internet, instead of synchronizing to online depots, you can configure vSphere Lifecycle Manager to download updates from an UMDS-created shared repository. When you configure vSphere Lifecycle Manager to use a UMDS repository, synchronization of the updates metadata is not triggered immediately. The metadata is downloaded according to the configured download schedule or when you initiate the download. When the default download source for vSphere Lifecycle Manager is a UMDS repository, only the metadata is stored and displayed in the vSphere Client. The actual payload is downloaded during staging or remediation.

Note:

The default online depot URLs are now unique for each customer. To update the default download URLs in the UMDS configuration files, see the following KB article: https://knowledge.broadcom.com/external/article/390123.

Depot Overrides

In ROBO scenarios, you can configure vSphere Lifecycle Manager to use a local depot with updates for a particular cluster instead of the depots that all clusters in that vCenter Server instance use by default.

For more information, see Manage Depot Overrides for a Cluster.

Browsing the vSphere Lifecycle Manager Depot

You can use the vSphere Client to view and browse the contents of the vSphere Lifecycle Manager depot.

You can view the vSphere Lifecycle Manager depot in the vSphere Lifecycle Manager home view. The contents of the vSphere Lifecycle Manager depot are displayed on three different tabs: **Image Depot**, **Updates**, and **Imported ISOs**.

Image Depot

On the **Image Depot** tab, you can view all VMware base images, vendor add-ons, and components that are available in the vSphere Lifecycle Manager depot.

You can use the **ESXi Versions**, **Vendor Addons**, and **Component** links at the top of the pane for easier navigation through the lists.

The **ESXi Versions** list contains all base images available in the depot together with information about the version, release date, and category for each image. When you select an image from the list, an information panel appears on the right. The panel displays a list of all components that the base image applies to a host upon remediation.

The **Vendor Addons** list contains all vendor addons available in the depot together with information about the version, release date, and category for each addon. When you select an add-on from the list, an information panel appears on the right. The panel displays information about the components that the add-on applies to the host and the components that the add-on removes from a host upon remediation.

The **Component** list contains all components that are available in the depot together with information about the version, release date, and category for each component. When you select a component from the list, an information panel appears on the right. The panel displays information about the VIBs that the component contains.

You can filter the **Component** list so that it displays only independent components or all components available in the vSphere Lifecycle Manager depot. Independent components are components that are not part of a vendor add-on.

You use the ESXi images, vendor add-ons, and components visible on the **Image Depot** tab to set up images that you can use to manage hosts in clusters collectively.

Updates

On the **Updates** tab, you can see all components available in the vSphere Lifecycle Manager depot as bulletins. You can use the **Filter by Baseline** drop-down menu to view only the bulletins that are part of a particular baseline.

When you select a bulletin from the list, additional information appears below the bulletins list. In the bottom pane, you see information about the baselines that include the selected bulletin.

You use the bulletins visible on the **Updates** tab to create baselines and baseline groups.

Because in vSphere 7.0 the official VMware depot hosts certified partner content in addition to VMware content, the **Updates** tab displays a broader set of OEM bulletins, for example vendor add-ons and VMware-certified device drivers. Some of these bulletins might have dependencies that must be pulled into the baselines that you create, so that the remediation against those baselines is successful. As a best practice, always consult the KB article for an individual bulletin to find information about its deployment specfics and reqired dependencies before including the bulletin in your

baselines. For more information about the official VMware depot and other types of depots, see vSphere Lifecycle Manager Download Sources.

Starting with vSphere 7.0, some changes are also introduced in the way VMware content is packaged. As a result, you might see additional bulletins on the **Updates** tab at patch and update releases. Those bulletins are usually of the Enhancement or BugFix category. When you include those bulletins in a baseline, you might need to also include a base ESXi bulletins in that baseline. As a best practice, to ensure successful application of patches and updates, always include the appropriate rollup bulletin into your baselines. You can use the **Show only rollup updates** toggle switch that is on the **Updates** tab to filter the list of bulletins.

Imported ISOs

On the **Imported ISOs** tab, you can see the ISO images that you import and make available to vSphere Lifecycle Manager.

You use the ISO images visible on the **Imported ISOs** tab to create upgrade baselines. You cannot use an ISO image for clusters configured to use a single vSphere Lifecycle Manager image.

Note: ISO images are not distributed through any online or offline depot, they are a separate software distribution format. As a result, they cannot become available in the vSphere Lifecycle Manager depot through synchronization or the regular import operation that you perform to import offline bundles (ZIP files) to the depot. To make an ISO image available to vSphere Lifecycle Manager, you must trigger the **Import ISO** operation. For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot

Import Updates to the vSphere Lifecycle Manager Depot

You can use an offline bundle in ZIP format and import updates to the vSphere Lifecycle Manager depot manually. When you import offline bundles, you add both the update metadata and actual payload to the vSphere Lifecycle Manager depot.

- Verify that the updates that you import are in ZIP format.
- Required privileges: **VMware vSphere Lifecycle Manager** > **Upload File** > **Upload File**.

You use the import option to populate the vSphere Lifecycle Manager depot with updates from an offline bundle. Offline bundles can contain patches and extensions. Starting with vSphere 7.0, an offline bundle can also contain an ESXi base image, a vendor add-on, or third-party software, for example, asynchronous drivers specific to the OEM hardware requirements. For more information about base images, vendor add-ons, and components, see Bulletins, Components, Add-Ons, and ESXi Base Images.

If you want to use vSphere Lifecycle Manager baselines, you can import offline bundles that contain patches and extensions for hosts that run ESXi 6.5 and later. In that case, you can use the contents of the offline bundle only for host patching operations. If you import an OEM offline bundle that contains an ESXi image of a version earlier than 7.0, you cannot use the image for upgrade operations. To create upgrade baselines, you need an ISO image. For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.

If you want to use vSphere Lifecycle Manager images, you can import offline bundles that contain software for hosts that run ESXi 7.0 and later. In that case, you can use the contents of the offline bundle to set up vSphere Lifecycle Manager images, which you can use to upgrade ESXi hosts collectively.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2. Select **Actions** > **Import Updates** at the top of the vSphere Lifecycle Manager home view.
   The **Import Updates** dialog box opens.
3. Enter a URL or browse to an offline bundle in ZIP format on your local machine.
   If the upload fails, check whether the structure of the ZIP file is correct and whether the vSphere Lifecycle Manager network settings are set up correctly.
4. Click **Import**.
   The Import updates task appears in the **Recent Tasks** pane.

You imported updates to the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager automatically generates new image recommendations for the clusters that already have generated recommended images. However, if the imported updates are solution components only, vSphere Lifecycle Manager does not generate new recommendations automatically.

You can view the imported patches and extension on the **Updates** tab in the vSphere Lifecycle Manager home view.

You can view the imported ESXi images, vendor add-ons, and additional components on the **Image Depot** tab in the vSphere Lifecycle Manager home view.

Import an ISO Image to the vSphere Lifecycle Manager Depot

You import ESXi images in ISO format to the vSphere Lifecycle Manager local depot, so that you can create upgrade baselines, which you use for host upgrade operations.

Required privileges: **VMware vSphere Lifecycle Manager** > **Upload File**

You can use ESXi`.iso` images to upgrade ESXi 6.5.x hosts and ESXi6.7.x hosts to ESXi7.0.

With vSphere Lifecycle Manager7.0, you cannot perform ESXi upgrades to version 6.7 or 6.5.

ISO images can only be used with vSphere Lifecycle Manager baselines. You cannot use an ISO image to upgrade the hosts in a cluster that uses a single image.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-7.0.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder. You can also use ISO images created and distributed by OEMs.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Imported ISOs** tab, click **Import ISO**
3. In the **Import ISO** dialog box, select an image.
   - Click the **Browse** button to import an ESXi image from your local system.
   - Enter an URL address to import an ESXi image that is not on your local system.

   Local images are imported immediately, whereas importing images from a URL takes some time.
4. Click **Import**.

The ISO image that you uploaded appears in the list of images. You can view information about the ESXi image, such as product, version, and build details, vendor, acceptance level, and creation date.

Create a host upgrade baseline.

Delete an ISO Image from the vSphere Lifecycle Manager Depot

If you do not need an ESXi image, you can delete it from the vSphere Lifecycle Manager depot.

- Verify that the ISO image that you want to delete is not part of any baseline. You cannot delete images that are included in a baseline.
- Delete any baseline that contains the ISO image that you want to delete.

Unlike components and bulletins, which you cannot delete from the vSphere Lifecycle Manager depot, the ISO images that you import in the depot can be deleted when you no longer need them .

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Imported ISOs** tab, select an image from the list and click **Delete**.

   Note: If you try to delete an ESXi image that is used in a baseline, the operation fails with an error message.
3. Click **Yes** to confirm the deletion.

The ISO image is deleted and no longer available.

Synchronize the vSphere Lifecycle Manager Depot

Instead of waiting for the predefined download task to run as scheduled, you can update your local vSphere Lifecycle Manager depot immediately.

At regular configurable intervals, vSphere Lifecycle Manager downloads updates from the configured download sources. The download sources can be online depots or a UMDS-created shared repository.

Regardless of the download schedule, you can initiate synchronization between the vSphere Lifecycle Manager depot and the configured download sources. Similar to scheduled synchronization, when you initiate synchronization manually, vSphere Lifecycle Manager downloads software from all online depots that you configured it to use. For more information about configuring the vSphere Lifecycle Manager download sources, see Configuring the vSphere Lifecycle Manager Download Sources.

During synchronization, vSphere Lifecycle Manager downloads only the update metadata, the actual payloads are downloaded during staging or remediation.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. Select **Actions** > **Sync Updates** at the top of the vSphere Lifecycle Manager home view.

   The Sync updates task appears in the **Recent Tasks** pane.

You downloaded updates to the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager automatically generates new image recommendations for the clusters that already have generated recommended images. However, if the updates are related to downloading solution components only, vSphere Lifecycle Manager does not generate new recommendations automatically.

You can view the downloaded patches and extension on the **Updates** tab in the vSphere Lifecycle Manager home view.

You can view the downloaded ESXi images, vendor add-ons, and components on the **Image Depot** tab in the vSphere Lifecycle Manager home view.

Configuring the vSphere Lifecycle Manager Download Sources

You can configure vSphere Lifecycle Manager to download software updates for ESXi hosts either from the Internet or from a shared repository of UMDS data.

vSphere Lifecycle Manager downloads only the metadata and not the actual binary payload of the updates. Downloading the metadata saves disk space and network bandwidth. The availability of regularly updated metadata in the vSphere Lifecycle Manager depot lets you perform compliance checks on hosts at any time.

Whatever the download source, vSphere Lifecycle Manager downloads the following types of information:

- Metadata about all ESXi 6.x updates regardless of whether you have hosts of such versions in your environment.
- Metadata about all ESXi 7.x updates regardless of whether you have hosts of such versions in your environment.
- Patch recalls for ESXi 6.x hosts.
  vSphere Lifecycle Manager supports the recall of patches for hosts that are running ESXi 6.5 or later. A patch is recalled when it has problems or potential issues. After you scan the hosts in your environment, vSphere Lifecycle Manager alerts you if the recalled patch has been installed on any host. Recalled patches cannot be installed on hosts with vSphere Lifecycle Manager. vSphere Lifecycle Manager deletes all the recalled patches from the vSphere Lifecycle Manager depot. After a patch that fixes the problem is released, vSphere Lifecycle Manager downloads the new patch to its depot. If you have already installed the problematic patch, vSphere Lifecycle Manager notifies you that a fix is available and prompts you to apply the new patch.

Downloading host patches from the Broadcom Support Portal Downloads website is a secure process.

- Download URLs for updates and patches are unique for each customer. For more information about the online depot URLs and how to edit the vSphere Lifecycle Manager configuration, see the following KB article: https://knowledge.broadcom.com/external/article/390121.
- Patches are cryptographically signed with the VMware private keys. Before you try to install a patch on a host, the host verifies the signature. This signature enforces the end-to-end protection of the patch itself and can also address any concerns about downloading the patch.
- vSphere Lifecycle Manager downloads the patch metadata and patch binaries over SSL connections. vSphere Lifecycle Manager verifies both the validity of the SSL certificates and the common name in the certificates. The common name in the certificates must match the names of the servers from which vSphere Lifecycle Manager downloads the patches. vSphere Lifecycle Manager downloads the patch metadata and binaries only after successful verification of the SSL certificates.

Download Sources

If your deployment system is connected to the Internet, you can use the default settings and links for downloading updates to the vSphere Lifecycle Manager depot. You can also add URL addresses to download third-party software, for example drivers.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the upgrades, patches, and extensions by using Update Manager Download Service (UMDS).

For more information about UMDS, see Installing, Setting Up, and Using Update Manager Download Service.

The default configuration is for the vSphere Lifecycle Manager to download information directly from the Internet. However, you can change the download source at any time. Changing the download source from a shared repository to the Internet and the reverse is a change in the vSphere Lifecycle Manager configuration. The two options are mutually exclusive. You cannot download updates from the Internet and a shared repository at the same time.

By default, vSphere Lifecycle Manager is configured to use the official VMware online depot as a download source. When you deploy vCenter Server, synchronization to the official VMware depot is triggered automatically. When you change the default download source, synchronization to the new download source is not triggered automatically. The synchronization task runs as per its schedule. To download new data, you must run the VMware vSphere Update Manager Download task or trigger synchronization manually.

The VMware vSphere Update Manager Download task is a scheduled task that runs at regular intervals. You can change the schedule, and you can also trigger the VMware vSphere Update Manager Download task independently of its schedule.

If the VMware vSphere Update Manager Download task is running when you apply the new configuration settings, the task continues to use the old settings until it finishes. The next time the download task starts, vSphere Lifecycle Manager uses the new settings.

Using a Proxy Server

Starting with vSphere 7.0, you cannot configure vSphere Lifecycle Manager to use a proxy server on its own. vSphere Lifecycle Manager uses the proxy settings of the vCenter Server instance where it runs.

In vSphere 6.7 and earlier, you can configure the proxy settings for Update Manager and use a proxy server to download updates metadata from the Internet.

Configure vSphere Lifecycle Manager to Use a Shared Repository as a Download Source

You can configure vSphere Lifecycle Manager to use a shared repository as a source for downloading ESXi images, vendor add-ons, and additional components.

- Create a shared repository by using UMDS and host the repository on a Web server or a local disk. For detailed information about exporting the upgrades, update binaries, and update metadata in Export the Downloaded Data.
- Verify that UMDS is of version compatible with the version of vSphere Lifecycle Manager that you are using. For more information about compatibility, see Compatibility Between UMDS and vSphere Lifecycle Manager.
- Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**.

You cannot use folders on a network drive as a shared repository. vSphere Lifecycle Manager does not download updates from folders on a network share in the Microsoft Windows Uniform Naming Convention form (such as `\\Computer_Name_or_Computer_IP\Shared`), or on a mapped network drive (for example, `Z:\`).

The downloading of updates takes place at configurable regular intervals. To initiate downloading of updates regardless of the download schedule, see Synchronize the vSphere Lifecycle Manager Depot .

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration** > **Patch Setup**.
3. Click the **Change Download Source** button.

   The **Change Download Source Type** dialog box opens.

4. Select the **Download patches from a UMDS shared repository** option and enter a path or URL address to the shared repository.
   For example, `C:\repository_path\`, `https://repository_path/` or `http://repository_path/`.

   In these examples, *`repository_path`* is the path to the folder with the exported downloaded upgrades, patches, extensions, and notifications. In an environment where vSphere Lifecycle Manager does not have direct access to the Internet, but is connected to a physical machine that has access to the Internet, the folder can be on a Web server.

   You can specify an HTTP or HTTPS address, or a location on the disk where vSphere Lifecycle Manager runs. HTTPS addresses are supported without any authentication.
5. Click **Save**.

   vCenter Server validates the URL. You can use the path to the shared repository only when the validation is successful. If the validation fails, vSphere Lifecycle Manager reports a reason for the failure.

   Important: If the updates in the folder that you specify are downloaded with a UMDS version that is not compatible with the vCenter Server version that you use, the validation fails and you receive an error message.

The shared repository is used as the main source for downloading software updates. Downloading from the repository is enabled by default.

Using a Folder or a Web Server as a Shared Repository

You can use a folder or a Web server as a shared repository.

- When you use a folder as a shared repository, *`repository_path`* is the path to the top-level directory that stores the patches and notifications exported from UMDS.
  For example, use UMDS to export the patches and notifications to the `F:\` drive, which is a drive mapped to a plugged-in USB device on the physical machine where UMDS is installed. Then, plug in the USB device to the physical machine where vSphere Lifecycle Manager runs. The device is mapped as `E:\` and the folder to configure as a shared repository for vSphere Lifecycle Manager is `E:\`.
- When you use a Web server as a shared repository, *`repository_path`* is the path to the top-level directory on the Web server that stores the patches exported from UMDS.
  For example, export the patches and notifications from UMDS to `C:\docroot\exportdata`. If the folder is configured on a Web server and is accessible from other physical machines at the URL `https://umds_host_name/exportdata`, the URL to configure as a shared repository in vSphere Lifecycle Manager is `https://umds_host_name/exportdata`.

Configure vSphere Lifecycle Manager to Use the Internet as a Download Source

If your deployment system is connected to the Internet, you can configure vSphere Lifecycle Manager to directly download ESXi images, vendor add-ons, and other components from the configured online depots to the local vSphere Lifecycle Manager depot.

Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**

The Internet is the default download source for vSphere Lifecycle Manager. Downloading takes place at configurable regular intervals. To initiate downloading of updates regardless of the download schedule, see Synchronize the vSphere Lifecycle Manager Depot .

Note:

The default download source URLs are now unique for each customer. To update the default download Internet sources, see the following KB article: https://knowledge.broadcom.com/external/article/390121.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration** > **Patch Setup**.
3. Click the **Change Download Source** button.

   The **Change Download Source Type** dialog box opens.
4. Select the **Download patches directly from the Internet** option and click **Save**.

Add a New Download Source

If you use the Internet as a download source for updates, you can add URL addresses to third-party online depots. vSphere Lifecycle Manager downloads software updates from all the online depots that you configured it to use. Update metadata are downloaded from the online depots to the local vSphere Lifecycle Manager depot.

Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**

The default download source for vSphere Lifecycle Manager is the official VMware depot.

Note:

The default download source URLs are now unique for each customer. To update the default download Internet sources, see the following KB article: https://knowledge.broadcom.com/external/article/390121.

Starting with vSphere 7.0, the official VMware online depot also hosts vendor add-ons and VMware-certified device drivers. Unlike previous releases, all software that you need to install, update, or customize the ESXi version of your hosts is available in the official VMware online depot.

Downloading updates takes place at configurable regular intervals. To initiate the downloading of updates regardless of the download schedule, see Synchronize the vSphere Lifecycle Manager Depot .

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration** > **Patch Setup**.
3. In the **Patches downloaded from the Internet** pane, click **New**.

   The **New Download Source** dialog box opens.
4. Enter a URL address to a new download source.

   vSphere Lifecycle Manager supports both HTTP and HTTPS URL addresses. Use HTTPS URL addresses to download data securely. The URL addresses that you add must be complete and contain an `index.xml` file, which lists the vendor and the vendor index.

   Note: The proxy settings that vSphere Lifecycle Manager uses are also applicable to third-party URL addresses.

5. Optional: Enter a short description for the download source.
6. Click **Save**.

The new location is added to the list of download sources and downloading from it is enabled by default.

Modify a Download Source

You can edit or delete a download source from the list of vSphere Lifecycle Manager download sources. You can also allow or disallow vSphere Lifecycle Manager to download updates from a particular download source.

Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration** > **Patch Setup**.
3. In the **Patches downloaded from the Internet** pane, select a URL address from the list of download sources and select your task.
   - Click **Edit** to edit the source URL or the description for the selected download source.
   - Click **Enable** or **Disable** to allow or disallow downloading from the selected download source.
   - Click **Delete** to delete the selected download source.

   Note: You cannot edit or delete the default VMware download source for ESXi updates. You can only allow or disallow vSphere Lifecycle Manager to use it for downloading update metadata from it.

Configure the vSphere Lifecycle Manager Automatic Download Task

Downloading host updates and related metadata is a predefined automatic process that you can modify. The automatic download task is enabled by default and starts immediately after you deploy vCenter Server. After the initial download, the task runs according to its schedule.

- Verify that the machine on which vSphere Lifecycle Manager runs has access to the Internet.
- Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**.

The default schedule settings ensure frequent checks, but you can change the schedule if your environment requires you to adjust the frequency of the checks.

If you need the latest software updates, you might want to reduce the time interval between the checks for updates. By contrast, if you are not concerned about the latest updates, if you want to reduce the network traffic, or if you cannot access the update servers, you might want to increase the time interval between the checks for updates.

The automatic download of update metadata is enabled by default and the default task name is VMware vSphere vSphere Lifecycle Manager Update Download. You can change the configuration of the task.

Note:

The default download source URLs are now unique for each customer. To update the default download Internet sources and avoid errors when the automatic download tasks are initiated, see the following KB article: https://knowledge.broadcom.com/external/article/390121.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration** > **Patch Downloads**.
3. In the **Automatic Download Settings** pane, click the **Edit** button.

   The **Edit Settings for Automatic Patch Downloads** dialog box opens.
4. Select the **Download patches** check box and configure the schedule and settings for the download.

   To receive notification emails after the download task finishes, you must configure mail settings for the vSphere Client. For more information, see the *vCenter Server and Host Management* documentation.
5. Click **Save** to save your changes and close the dialog box.

The automatic download task runs according to the schedule you configured.

Run the VMware vSphere vSphere Lifecycle Manager Update Download Task

If you change the download source, you must run the VMware vSphere vSphere Lifecycle Manager Update Download task to download any new updates.

1. In the vSphere Client, navigate to a vCenter Server instance.
2. On the **Configure** tab, select **Scheduled Tasks**.
3. In the **Scheduled Tasks** pane, select the **VMware vSphere Lifecycle Manager Update Download** task and click **Run**.

You can see the running task listed in the **Recent Tasks** pane.

Configuring the vSphere Lifecycle Manager Remediation Settings

Whether you manage the ESXi hosts in your environment with baselines or with images, you can configure the behavior of vSphere Lifecycle Manager during host update and upgrade operations.

You can configure and modify the vSphere Lifecycle Manager settings only if you have the privileges to configure the vSphere Lifecycle Manager settings and service. The permission must be assigned to the vCenter Server where vSphere Lifecycle Manager runs. For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation. For a list of the vSphere Lifecycle Manager privileges and their descriptions, see Privileges for Using vSphere Lifecycle Manager Images and Baselines.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can configure the settings for each vSphere Lifecycle Manager instance. The configuration properties that you modify are applied only to the vSphere Lifecycle Manager instance that you specify, and are not propagated to the other instances in the domain.

You can change any of the vSphere Lifecycle Manager settings on the **Settings** tab in the vSphere Lifecycle Manager home view.

Host Remediation Settings

You can use baselines or images to remediate individual hosts or all hosts in a cluster collectively. Some remediation settings are applicable regardless of whether you use baselines or images to initiate host remediation. For example, you can configure virtual machine migration settings, maintenance mode settings, and quick boot for hosts that are managed by either cluster images or baselines.

Other settings are applicable only to hosts that you manage by using baselines and baselines groups. Such settings are allowing the installation of software on PXE booted hosts and the removal of media devices before maintenance mode.

For information about how to configure host remediation settings, see Configure Remediation Settings for vSphere Lifecycle Manager Baselines and Configure Remediation Settings for vSphere Lifecycle Manager Images .

You can also configure certain cluster settings to ensure successful remediation. For more information about the cluster settings that affect host remediation, see Cluster Settings and Host Remediation.

Cluster Settings and Host Remediation

When you remediate ESXi hosts that are in a cluster, certain cluster settings might cause remediation failure. You must configure the cluster settings in such a way as to ensure successful remediation.

When you update the ESXi hosts in a cluster that has vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), and vSphere Fault Tolerance (FT) activated, you can temporarily deactivate vSphere Distributed Power Management (DPM), HA admission control, and FT for the entire cluster. When the update finishes, vSphere Lifecycle Manager restarts these features.

DRS

Updates might require a host to enter maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, you can activate DRS for the cluster and you can configure it for vSphere vMotion. In this case, before the host is put in maintenance mode, vCenter Server migrates the virtual machines to another ESXi host within the cluster.

To help ensure vSphere vMotion compatibility between the hosts in the cluster, you can activate Enhanced vMotion Compatibility (EVC). EVC ensures that all hosts in the cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. EVC prevents migration failures due to incompatible CPUs. You can use EVC only in a cluster where the host CPUs meet the compatibility requirements. For more information about EVC and the requirements that the hosts in an EVC cluster must meet, see the *vCenter Server and Host Management* documentation.

DPM

If a host has no running virtual machines, DPM might put the host in standby mode, which might interrupt a vSphere Lifecycle Manager operation. So, to make sure that all vSphere Lifecycle Manager operations finish successfully, you can configure vSphere Lifecycle Manager to deactivate DPM during these operations. For successful remediation, you must have vSphere Lifecycle Manager deactivate DPM. After the remediation task finishes, vSphere Lifecycle Manager restores DPM.

If DPM has already put a host in standby mode, vSphere Lifecycle Manager powers on the host before compliance checks and remediation. Additionally, for clusters that you manage with baselines, vSphere Lifecycle Manager powers on the host before staging, too. After the respective task finishes, vSphere Lifecycle Manager turns on DPM and HA admission control and lets DPM put the host into standby mode, if needed. vSphere Lifecycle Manager does not remediate powered off hosts.

If a host is put in standby mode and DPM is manually deactivated for a reason, vSphere Lifecycle Manager does not remediate or power on the host.

HA Admission Control

Within a cluster, you must deactivate HA admission control temporarily to let vSphere vMotion proceed. This action prevents downtime for the machines on the hosts that you remediate. You can configure vSphere Lifecycle Manager to deactivate HA admission control during remediation. After the remediation of the entire cluster is complete, vSphere Lifecycle Manager restores the HA admission control settings. vSphere Lifecycle Manager deactivates HA admission control before remediation, but not before compliance checks. Additionally, for clusters that you manage with baselines, vSphere Lifecycle Manager deactivates HA admission control before staging.

Disabling HA admission control before you remediate a two-node cluster that uses a single vSphere Lifecycle Manager image causes the cluster to practically lose all its high availability guarantees. The reason is that when one of the two hosts enters maintenance mode, vCenter Server cannot failover virtual machines to that host and HA failovers are never successful. For more information about HA admission control, see the *vSphere Availability* documentation.

Fault Tolerance

If FT is turned on for any of the virtual machines on a host within a cluster, you must temporarily turn off FT before performing any vSphere Lifecycle Manager operation on the cluster. If FT is turned on for any of the virtual machines on a host, vSphere Lifecycle Manager does not remediate that host. You must remediate all hosts in a cluster with the same updates, so that FT can be reactivated after remediation. A primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESXi versions and patch levels.

Configure Remediation Settings for vSphere Lifecycle Manager Images

You can configure how ESXi hosts and VMs behave before and during the remedition of a cluster that you managed with a single image.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

When you edit images remediation settings, you set the global remediation setting for all clusters that you manage with images. However, you can override the global remedation settings and use specific remediation settings for a cluster. For more information, see Edit the Remediation Settings for a Cluster.

Hosts that are in a vSAN cluster can enter maintenance mode only one at a time. This behavior is a peculiarity of the vSAN cluster. For more information about the vSphere Lifecycle Manager behavior during the remediation of hosts in a vSAN cluster, see Remediation Specifics of vSAN Clusters .

For information about automatically triggered hardware compatibility checks, which is a functionality that is also applicable only to vSAN clusters, see Automatically Triggered Hardware Compatibility Checks for vSAN Clusters.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Host Remediation** > **Images**.
3. Click the **Edit** button.

   The **Edit Cluster Settings** dialog box opens.
4. Configure the images remediation settings and click **Save**.

Option	Description
Quick Boot	Quick Boot reduces the host reboot time during remediation. Before you enable Quick Boot, you must ensure that the ESXi host is compatible with the feature.

Option	Description
	By default, Quick Boot is turned off.
VM power state	The **VM power state**option lets you control the behavior of the virtual machines that run on the ESXi host. You can select from the following options. • **Do not change power state** • **Suspend to disk** • **Suspend to memory** To select the **Suspend to memory** option, you must enable Quick Boot. Otherwise, the **Suspend to memory** option is dimmed. Together with Quick Boot, the **Suspend to memory** option provides faster host upgrades. vSphere Lifecycle Managersuspends to the host memory and not to the disk the powered on virtual machines on the host. After the Quick Boot, the suspended virtual machines are resumed from memory. • **Power off** The default selection is **Do not change power state**.
VM migration	You can configure vSphere Lifecycle Manager to migrate the suspended and powered off virtual machines from the hosts that must enter maintenance mode to other hosts in the cluster. The default configuration is set to **Do not migrate powered off and suspended VMs to other hosts in the cluster**.
Maintenance mode failures	You can configure how vSphere Lifecycle Manager behaves if a host fails to enter maintenance mode before remediation. You can configure vSphere Lifecycle Manager to wait for a specified retry delay period and to retry to put the host into maintenance mode as many times as you indicate in the **Number of retries** text box.
HA admission control	Admission control is a policy that vSphere HA uses to ensure failover capacity within a cluster. If vSphere HA admission control is enabled during remediation, vMotion might be unable to migrate the virtual machines within the cluster. Disabling admission control allows a virtual machine to be powered on even if it causes insufficient failover capacity. When this happens, no warnings are presented, and the cluster does not turn red. If a cluster has insufficient failover capacity, vSphere HA can still perform failovers, and uses the VM Restart Priority setting to determine which virtual machines to power on first. • If you select the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables HA admission control after remediation is complete. • If you deselect the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which HA admission control is enabled.

Option	Description
	By default, the **Disable HA admission control on the cluster** option is deselected.
DPMvsa	VMware Distributed Power Management (DPM) monitors the resources consumed by the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. • If you select the **Disable DPM on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables DPM after remediation is complete. • If you deselect the **Disable DPM on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which DPM is enabled. By default, the **Disable DPM on the cluster** option is enabled.
Hardware compatibility issues	vSphere Lifecycle Manager performs a hardware compatibility check as part of the remediation pre-check and the remediation tasks for vSAN clusters. You can configure vSphere Lifecycle Manager to prevent remediation when hardware compatibility issues exist for the cluster. • If you select the **Prevent remediation if hardware compatibility issues are found** option, vSphere Lifecycle Manager reports hardware compatibility issues as an error, which prevents remediation. • If you deselect the **Prevent remediation if hardware compatibility issues are found** option, vSphere Lifecycle Manager reports hardware compatibility issues as a warning, which does not prevent remediation. If the cluster is not vSAN-enabled, vSphere Lifecycle Manager does not perform a hardware compatibility check as part of the remediation pre-check or the remediation tasks.

These settings become the default failure response settings with vSphere Lifecycle Manager images. You can specify different settings when you configure individual remediation tasks.

Configure Remediation Settings for vSphere Lifecycle Manager Baselines

You can configure how vSphere Lifecycle Manager behaves before and during remediation against a baseline or a baseline group. The remediation settings help ensure that vSphere Lifecycle Manager puts ESXi hosts in maintenance mode before remediation.

Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**

vSphere Lifecycle Manager might behave differently during remediation against an image and against a baseline.

You cannot use vMotion to migrate virtual machines that run on individual hosts. If vCenter Server cannot migrate the virtual machines to another host, you can configure how vSphere Lifecycle Manager responds. You can also configure how vSphere Lifecycle Manager responds when a host fails to enter maintenance mode.

Hosts that are in a vSAN cluster can enter maintenance mode only one at a time. This behavior is a peculiarity of the vSAN cluster. For more information about the vSphere Lifecycle Manager behavior during the remediation of hosts in a vSAN cluster, see vSAN Clusters and vSphere Lifecycle Manager.

When you use vSphere Lifecycle Manager baselines, you can configure vSphere Lifecycle Manager to let other software initiate the remediation of PXE booted ESXi hosts. The remediation installs software modules on the hosts, but typically those host updates are lost after a reboot. To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with vSphere Lifecycle Manager, so that the updates are not lost because of a reboot. vSphere Lifecycle Manager itself does not reboot the hosts, because it does not install updates requiring a reboot on PXE booted ESXi hosts.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Host Remediation** > **Baselines**.
3. Click the **Edit** button.

   The **Edit Settings for Host Remediation** dialog box opens.
4. Configure the baselines remediation settings and click **Save**.

Option	Description
VM power State	You can configure vSphere Lifecycle Manager to power off or suspend all running virtual machines before host remediation. Alternatively, you can configure vSphere Lifecycle Manager not to change the power state of the virtual machines.
Maintenance mode failures	You can configure how vSphere Lifecycle Manager behaves if a host fails to enter maintenance mode before remediation. If you enable vSphere Lifecycle Manager to retry to put the host in maintenance mode, you must specify the number of retries and the retry delay. vSphere Lifecycle Manager waits for as much time as you configure for the **Retry Delay** option, and retries to put the host in maintenance mode as many times as you indicate in the **Number of retries** text box.
PXE booted hosts	You can allow the installation of software for solutions on the PXE booted ESXi hosts in the vSphere inventory that you manage with vSphere Lifecycle Manager baselines.
VM migration	If you enable virtual machine migration by selecting the respective option, vSphere Lifecycle Manager migrates the suspended and powered off virtual machines from the hosts that must enter maintenance mode to other hosts in the cluster.
Removable media devices	vSphere Lifecycle Manager does not remediate hosts on which virtual machines have connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host might prevent the host from entering maintenance mode and interrupt remediation. So, you can disconnect all removable media devices to ensure that the respective host enters maintenance mode

Option	Description
	successfully. After remediation, vSphere Lifecycle Manager reconnects the removable media devices if they are still available.
Quick Boot	Quick Boot reduces the host reboot time during remediation. Before you enable Quick Boot, you must ensure that the ESXi host is compatible with the feature. For more information, see Quick Boot.
Parallel remediation	Enabling parallel remediation allows you to remediate multiple ESXi hosts simultaneously. By selecting the **Parallel remediation** option, you enable vSphere Lifecycle Manager to remediate all hosts that are in maintenance mode in parallel instead of in sequence. Alternatively, you can specify the maximum number of concurrent remediations manually. If the hosts have NSX virtual distributed switches that are ready to be migrated to vSphere Distributed Switches, you must manually set the maximum number of parallel remediations to no more than 4. In cases when host switch migration is needed, if more than 4 hosts are remediated in parallel, the remediation might fail, because the host switch migration takes more time than the time vSphere Lifecycle Manager needs to complete the parallel remediation.

These settings become the default failure response settings with vSphere Lifecycle Manager baselines. You can specify different settings when you configure individual remediation tasks.

Configuring vSphere Lifecycle Manager for Fast Upgrades

During cluster or host remediation, you can preserve the state of the virtual machines in the host memory and restore them from memory after the remediation finishes. Suspending virtual machines to memory and using the Quick Boot functionality significantly reduces the time for remediation, minimizes system boot time, and reduces the downtime of system and services.

During remediation with vSphere Lifecycle Manager, migrating virtual machines from the host that is under remediation to another host takes a considerable amount of time. After remediation, vSphere Lifecycle Manager migrates back the virtual machines to the remediated host. However, you can configure vSphere Lifecycle Manager to suspend virtual machines to memory instead of migrating them, powering them off, or suspending them to disk.

You can use the suspend to memory functionality only for patching operations, for example, when you remediate a cluster to apply to it a hot patch, express patch, and so on. You cannot use the suspend to memory option for upgrade operations, for example when you upgrade your ESXi hosts from version 7.0 Update 2 to 7.0 Update 3.

Suspend Virtual Machines to Memory

Suspend to memory is an option that you can use only for clusters that you manage with vSphere Lifecycle Manager images. The functionality works together with the Quick Boot setting to optimize the remediation process and minimize virtual machine downtime.

You enable vSphere Lifecycle Manager to suspend virtual machines to memory when you configure the vSphere Lifecycle Manager host remediation settings. During remediation pre-check and remediation, vSphere Lifecycle Manager verifies that the suspend to memory option is indeed applicable to the host or cluster under remediation. If for some reason suspend to memory is inapplicable, vSphere Lifecycle Manager reports an error and prevents remediation from proceeding.

During a suspend to memory operation, virtual machines remain in a suspended state for some time. So, suspending virtual machines to memory might impact the workloads running on those virtual machines. The impact is similar to the impact that the suspend to disk operation might have on virtual machines and workloads.

CAUTION: As a best practice, always take snapshots of the virtual machines with critical workloads before you start remediation when the suspend to memory option is activated.

vSphere Lifecycle Manager might not suspend to memory all virtual machines on the host even if you activated the feature for the entire cluster. In some cases, vSphere Lifecycle Manager is still able to proceed with the remediation of the host, even if some virtual machines cannot be suspended to memory.

- vSphere ESX Agent Manager (EAM) virtual machines
  vSphere Lifecycle Manager powers off the EAM virtual machines after all other virtual machines are suspended. Similarly, vSphere Lifecycle Manager powers on the EAM virtual machines before any other virtual machines are resumed from memory. None of the suspended virtual machines is resumed until the EAM virtual machines are powered on.
- vSphere Cluster Services virtual machines
  vSphere Lifecycle Manager first migrates to another host the vSphere Cluster Services virtual machines, and then suspends to memory the rest of the virtual machines on the host.

Similarly, vSphere Lifecycle Manager does not suspend to memory the management virtual appliances for some VMware products and solutions. However, if a virtual machine for any of the following products or solutions runs on a host, the suspend to memory pre-check fails and vSphere Lifecycle Manager does not proceed with the remediation of the respective host:

- vCenter Server
- vSAN witness virtual machine
- vSphere with Tanzu
- NSX-T Data Center
- VMware HCX
- vSphere Replication
- Site Recovery Manager
- VMware vRealize products

Note: Third-party virtual machines do get suspended during remediation, if the Suspend to memory option is activated.

Quick Boot

Quick Boot is a setting that you can use with clusters that you manage with vSphere Lifecycle Manager images and vSphere Lifecycle Manager baselines. Using Quick Boot optimizes the host patching and upgrade operations. Quick Boot lets vSphere Lifecycle Manager reduce the remediation time for hosts that undergo patch and upgrade operations. Patch and upgrade operations do not affect the hardware of a host. If the Quick Boot feature is activated, vSphere Lifecycle Manager skips the hardware reboot (the BIOS or UEFI firmware reboot). As a result, the time an ESXi host spends in maintenance mode is reduced and the risk of failures during remediation is minimized.

To configure vSphere Lifecycle Manager to suspend virtual machines to the host memory, you must activate Quick Boot. However, you can activate Quick Boot even if you decide not to use the Suspend to memory option.

Quick Boot is supported on a limited set of hardware platforms and drivers. Quick Boot is not supported on ESXi hosts that use TPM or passthrough devices. For more information about a host's compatibility with the Quick Boot setting, see the following KB article: https://kb.vmware.com/s/article/52477.

Requirements for Using Suspend to Memory

Several factors might hinder the applicability of the suspended to memory option. If for some reason suspend to memory is inapplicable, vSphere Lifecycle Manager reports an error and prevents remediation from proceeding. Suspend to memory works under the following conditions:

- The host supports the suspend to memory functionality.
- Quick Boot is activated for the cluster and the host under remediation supports Quick Boot.
- The remediation does not involve host upgrades or firmware upgrade.
- The host and the virtual machines meet certain requirements.

Host Requirements	Virtual Machine Requirements
• The host has enough free memory. • The host has sufficient free low memory. • The host has enough free memory per NUMA node to start after a reboot. • The host has enough reservation available • The host does not use swapped or compressed pages of virtual machines.	• The virtual machines do not have any passthrough devices. • The virtual machines do not have latency sensitivity set to high. • The virtual machines are not fault tolerant. • The virtual machines are not encrypted. • The virtual machines do not use persistent memory. • The virtual machines do not have virtual SGX or SEV devices. • The virtual machines do not have the suspend feature deactivated. • The virtual machines are not frozen source virtual machines during an Instant Clone operation.

Suspend to Memory and vSphere High Availability (HA)

When you configure vSphere Lifecycle Manager to suspend virtual machines to memory during remediation, vSphere HA provides protection for the suspended virtual machines in cases of failure at the virtual machine or host level. By modifying the vSphere HA advanced options, you can set a timeout value for suspended to memory virtual machines. If a suspended to memory virtual machine is not responsive for the specified time, vSphere HA powers on the virtual machine on the original host or on another host.

- If you deactivate or reconfigure vSphere HA for the cluster during remediation, vSphere HA can no longer protect the suspended virtual machines. Before you change the vSphere HA configuration, make sure that no hosts in the cluster are in maintenance mode and the suspended virtual machines are powered on.
- If you modify the `das.failoverDelayForSuspendToMemoryVmsSecs` advanced option for vSphere HA after you configure vSphere Lifecycle Manager to use the suspend to memory option, the newly specified timeout value might not apply to the virtual machines. If you need to modify the default value of the `das.failoverDelayForSuspendToMemoryVmsSecs` option, ensure that you modify it before you start remediation to ensure that the new value is in effect.
- If the suspend to memory operation fails, vSphere HA determines the most appropriate failover host after the specified timeout value expires. The failover host might be the original host or another one.
- You must synchronize the server time for all ESXi hosts in the cluster. If the hosts are not synchronized, vSphere HA might not respect the specified timeout period and initiate failover earlier or later.

For more information about using and configuring vSphere HA, see the *vSphere Availability* documentation.

Creating vSphere Lifecycle Manager Clusters

A vSphere Lifecycle Manager cluster is a cluster of ESXi hosts that you manage either with baselines or with a single image. You decide whether to manage a cluster with baselines or with a single image during the creation of the cluster.

Creating a vSphere Lifecycle Manager Cluster That Uses a Single Image

To create a cluster that uses a single image, you must select the respective option in the **Create Cluster** wizard and specify an image to be applied to the hosts. You can choose to create the image or to use an existing image from a host within or outside the current vCenter Server instance.

- Compose an image manually
  To set up an image manually, the vSphere Lifecycle Manager depot must contain the ESXi base image and vendor add-on that you want to use.
- Import an image from a reference host
  Starting with vSphere 7.0 Update 2, during cluster creation, you can select a reference host and use the image on that host as the image for the newly created cluster. vSphere Lifecycle Manager extracts the image from the reference host and applies it to the cluster.

Creating a vSphere Lifecycle Manager Cluster That Uses Baselines

To create a cluster that uses baselines, during cluster creation, you must leave unselected the option to manage the cluster with a single image. You can switch from using baselines to using images at a later time. For more information about switching from using baselines to using images, see Switching from Using Baselines to Using Images.

Adding Hosts to a vSphere Lifecycle Manager Cluster

You can add hosts of any version to a cluster that you manage with baselines.

You can add hosts of ESXi version 7.0 or later to a cluster that you manage with a single image. Starting with vSphere 7.0 Update 2, you can add a host to a cluster and at the same time use the image on that host as an image for the entire cluster.

Removing Hosts from a vSphere Lifecycle Manager Cluster

Removing a host from a cluster is a straightforward procedure. If you remove a host from a cluster that uses a single image, the host retains the software and firmware installed during the last remediation against the image for the cluster.

Note: When you remove a host from a vSAN cluster that you manage with a single image, vSphere Lifecycle Manager invalidates the results from the last hardware compatibility check for the cluster. To obtain valid hardware compatibility information about the cluster, you must re-run a hardware compatibility check. For instructions on how to check the hardware compatibility for a cluster, see Check the Hardware Compatibility of a Cluster .

All cluster-related operations are described in full detail in the *vCenter Server and Host Management* documentation.

For information about using Auto Deploy to deploy and provision ESXi hosts, see the *VMware ESXi Installation and Setup* documentation.

Create a Cluster That Uses a Single Image by Composing an Image Manually

You create a vSphere Lifecycle Manager cluster that uses a single image by setting up the desired image during the creation of the cluster. When you choose to set up the image manually instead of importing it from a host, you must have the necessary software available in the vSphere Lifecycle Manager depot.

- Review the requirements for using a single image in System Requirements for Using vSphere Lifecycle Manager.
- Verify that the hosts are of ESXi version 7.0 or later.
- Verify that a data center exists in the vCenter Server inventory.

- Verify that you have an ESXi image available in the vSphere Lifecycle Manager depot.

When you set up an image manually, you must specify the ESXi version for the image and, optionally, a vendor add-on. After the cluster creation is complete, you can further customize the image. For example, you can add components to the image. You can also configure a hardware support manager and add a firmware and drivers add-on to the image.

1. In the vSphere Client, navigate to the **Hosts and Clusters** inventory.
2. Right-click a data center and select **New Cluster**.
   The **New Cluster** wizard opens.
3. On the **Basics** page, enter a name for the cluster and enable vSphere DRS, vSphere HA, or vSAN.
4. Select the **Manage all hosts in the cluster with a single image** option.
5. Select the **Compose a new image** radio button and click **Next**.
6. On the **Image** page, set up the desired image and click **Next**.
   a) Select an ESXi version.
   b) Optional: Select a vendor add-on and the version of the add-on.
7. On the **Review** page, review your selections and the image setup.
8. Click **Finish** to finish the creation of the cluster.

A cluster that uses a single image appears in the vCenter Server inventory. You can view and customize the cluster image on the **Updates** tab for the cluster.

Add hosts to the cluster.

Create a Cluster That Uses a Single Image by Importing an Image from a Host

During cluster creation, instead of composing a new image, you can import the desired software specification from a reference host. If you choose to import an image, vSphere Lifecycle Manager extracts the software specification from the reference host and uses it for the newly created cluster. Importing an image saves you the time and effort of ensuring that you have all necessary components and images available in the vSphere Lifecycle Manager depot. Also, because you use a ready-made image, you do not need to spend time validating the new image.

- Verify that the vCenter Server version is 7.0 Update 2
- Verify that a data center exists in the vCenter Server inventory.
- Verify that the reference host is version ESXi 7.0 Update 2 or later.
- Obtain the user name and password of the root user account for the reference host if it is not in your vCenter Server instance.
- Review the requirements for using a single image in System Requirements for Using vSphere Lifecycle Manager.

During image import, along with extracting the software specification from the reference host, vSphere Lifecycle Manager also extracts the software depot associated with the image, and imports the software components to the vSphere Lifecycle Manager depot in the vCenter Server instance where you create the cluster. As a result, in air-gap scenarios, you only need one reference host to obtain the necessary ESXi image and components in the local depot and to create a software specification for your clusters.

You can import an image from an ESXi host that is in the same or a different vCenter Server instance. You can also import an image from an ESXi host that is not managed by vCenter Server. The reference host can also be in a cluster that you manage with baselines. Along with importing the image, you can also choose to move the reference host to the cluster. As a result, the newly created cluster uses the same image as the image on the reference host, which is now part of that cluster. But, if the reference host is in another vCenter Server instance, you can import the image from that host, but you cannot move it to the cluster.

Note: When you import an image from a host, vSphere Lifecycle Manager retrieves the ESXi version, vendor add-on, and user-added components from the host. vSphere Lifecycle Manager does not extract the components from solutions and firmware updates installed on the reference host. Therefore, the image for the new cluster does not contain solution components or a firmware and drivers add-on. To obtain firmware updates in the depot and add a firmware and drivers add-on to your cluster image, you must configure a hardware support manager for the cluster after the cluster is created. For more information about firmware updates, see Firmware Updates.

1. In the vSphere Client, navigate to the **Hosts and Clusters** inventory.
2. Right-click a data center and select **New Cluster**.
   The **New Cluster** wizard opens.
3. On the **Basics** page, enter a name for the cluster and enable vSphere DRS, vSphere HA, or vSAN.
4. Select the **Manage all hosts in the cluster with a single image** check box.
5. Choose the method of creating an image for the cluster and click **Next** .
   - To import an image from a host that is in the same vCenter Server inventory, select the **Import image from an existing host in vCenter inventory** radio button.
   - To import an image from a host that is in a different vCenter Server instance or a standalone host that is not added to a vCenter Server, select the **Import image from a new host** radio button.
6. Follow the prompts to complete the wizard.

Selected Import Option	Steps
Import image from an existing host in vCenter inventory	1. On the **Image** page, select the reference host which you want to extract the image from and click **Next**. **Note:** After you select a reference host, detailed information about the image on the selected host appears at the bottom of the page. You can view the ESXi version and all additional components. 2. On the **Review** page, review your selections and ensure that the selected reference host and its image are what you need. 3. Click **Finish**.
Import image from a new host	1. On the **Image** page, enter the host details and click the **Find Host** button. 2. If a **Security Alert** dialog box appears, click **Yes** to confirm that you want to connect to the host. 3. To move the host to the cluster, select the **Also move selected host to cluster** check box and click **Next**. 4. On the **Review** page, review your selections and verify that the selected reference host and its image are what you need. 5. Click **Finish**.

A cluster that uses a single image appears in the vCenter Server inventory. Depending on your selections, the reference host might be in the newly created cluster. The image for that cluster is identical to the image on the selected reference host. You can view and customize the cluster image on the **Updates** tab for the cluster.

Add other hosts to the cluster.

Add Hosts to a Cluster that Uses a Single Image

Starting with vSphere 7.0 Update 2, when you add hosts to a cluster, you can appoint one of those hosts as a reference host. vSphere Lifecycle Manager extracts and uses the image on the reference host as the new image for the cluster. The option to import a host's image to the cluster facilitates and simplifies the cluster upgrade operation by removing the

need for you to manually import components to the vSphere Lifecycle Manager depot, set up and validate a new image, check the compliance of the hosts against the image, and then remediate the cluster against the image to apply the new software specification to all hosts.

- Verify that the vCenter Server version is 7.0 or later.
- Verify that the hosts to add are of version ESXi 7.0 or later.
- Verify that the hosts that you add to the cluster are of the same main and patch version as the rest of the hosts.
- Obtain the user name and password of the root user account for the hosts that are not in your vCenter Server instance.
- Review the requirements for using a single image in System Requirements for Using vSphere Lifecycle Manager.
- To add a host and import its image to the cluster, verify that the following requirements are met.
  - The vCenter Server instance is of version 7.0 Update 2 or later
  - The ESXi version on the reference host is 7.0 Update 2 or later

Along with extracting the software specification from the appointed reference host, vSphere Lifecycle Manager also extracts the software depot associated with the image, and imports the components to the vSphere Lifecycle Manager depot in the vCenter Server instance where the target cluster is.

Note: When you import an image from a host, vSphere Lifecycle Manager retrieves the ESXi version, vendor add-on, and user-added components from the host. vSphere Lifecycle Manager does not extract the components from solutions and firmware updates installed on the reference host. Therefore, the new image for the cluster does not contain solution components or a firmware and drivers add-on. To obtain firmware updates in the depot and add a firmware and drivers add-on to your cluster image, you must configure a hardware support manager. For more information about firmware updates, see Firmware Updates.

Adding a host to a cluster and importing its image to the target cluster changes the compliance state of the other hosts in the cluster. After adding the host and setting its image as the new cluster image, you can run a compliance check. The newly added host is compliant against the new cluster image. The rest of the hosts become non-compliant. To apply the new cluster image to all the hosts in the cluster and make them compliant, you must remediate the cluster.

Note: You cannot downgrade the software that is actually installed on the hosts in the cluster. If the image on the reference host contains software components of lower version, you can still import and use that image for the cluster. However, the hosts in the cluster become incompatible with the new image, and you cannot proceed and remediate the cluster against that image.

1. In the vSphere Client, navigate to the **Hosts and Clusters** inventory.
2. Right-click cluster and select **Add Hosts**.

   The **Add Hosts** wizard opens.
3. On the **Add hosts**, specify the hosts that you want to add to the cluster and click **Next**.
   - Add a host that is not in the same vCenter Server inventory.
     a. Click the **New Hosts** tab.
     b. Enter the required information about the host in the text boxes.
     c. To add more new hosts, click the **Add Host** button and enter the required information.
     d. Select the **Use the same credentials for all hosts** check box.
   - Add a host that is in the same vCenter Server inventory.
     a. Click the **Existing hosts** tab.
     b. Select one or multiple hosts from the list.

   Note: If you want to add multiple hosts, you do not need to specify only new hosts or only existing hosts. You can specify new hosts and select from the existing hosts at the same time.

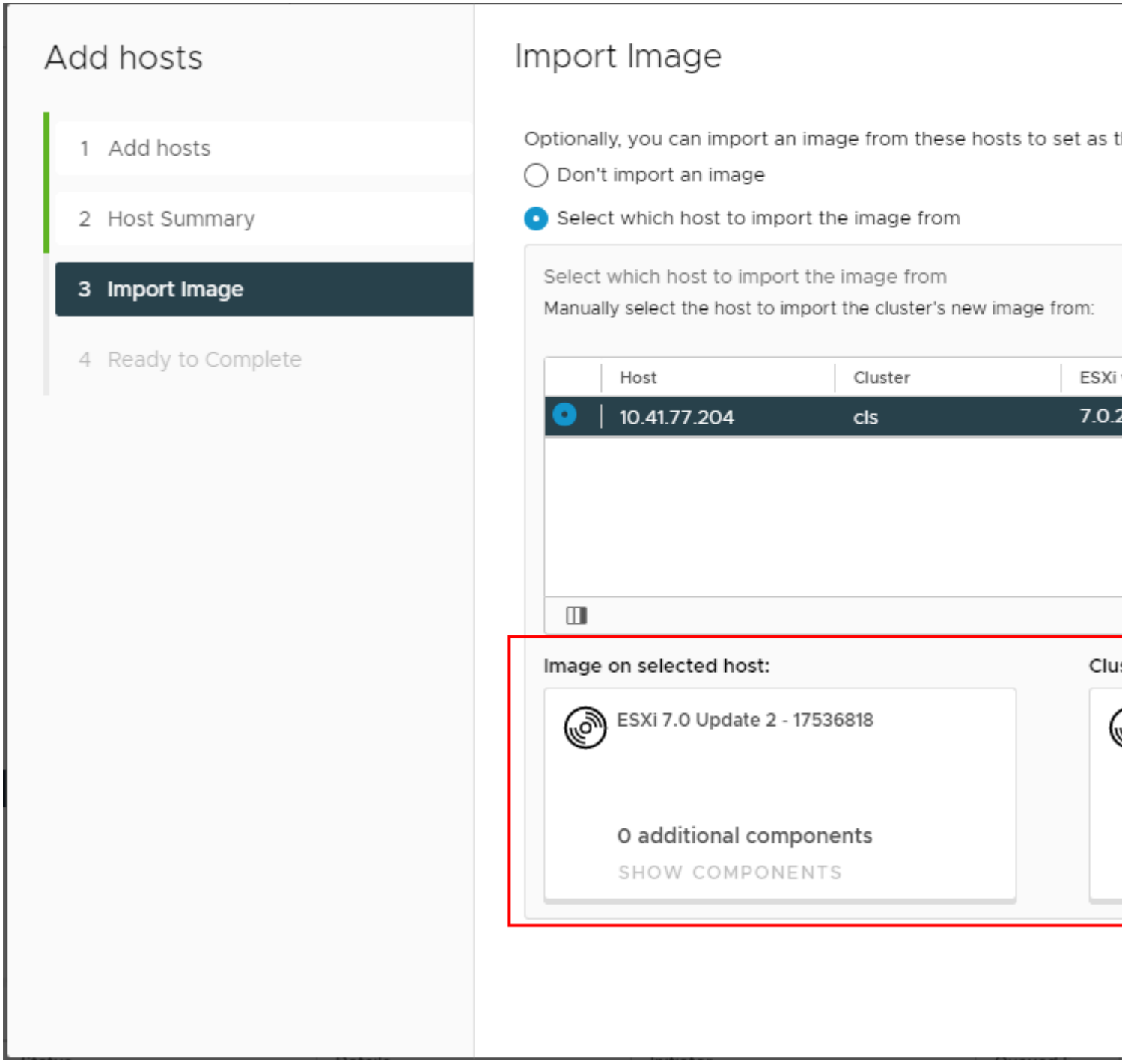
4. On the **Host Summary** page, review the information about the hosts and click **Next**.
5. On the **Import Image** page, select the host whose image to use as the image for the cluster.
   - To add the specified hosts to the cluster without changing the current image for that cluster, select the **Don't import an image** radio button.
   - To use any of the specified hosts as a reference host and use its image as the new image for that cluster, select the **Select which host to import the image from** radio button and select a host from the list.

     Note: If the image on the host that you select is of version earlier than ESXi 7.0 Update 2, you cannot proceed with importing the image from that host.

   When you select a host to import an image from, a card with information about the image appears. you can view the ESXi version, the vendor add-on, and the additional components that the image on the reference host contains.
6. If you selected the **Select which host to import the image from** radio button, click **Show Cluster's Current Image** at the bottom of the page.

   A card with information about the current image for the cluster appears. Before you proceed, you can review and compare the current cluster image with the image on the selected host

before you proceed. In this way, you can ensure that you selected the right reference host.



7. Click **Next**.
8. On the **Ready to Complete** page, review the information about the selected hosts and the new cluster image.
9. Click **Finish** to add the hosts to the cluster.

The specified hosts are added to the cluster.

If you chose to import an image from a host during the host addition procedure, the image for the cluster changes. The new software specification for the cluster is identical to the one on the selected and added reference host.

If you chose to import an image from a host during the host addition procedure, remediate the cluster to apply the new image to all the hosts.

Using vSphere Lifecycle Manager Baselines and Baseline Groups

Using baselines and baseline groups to manage the updates and upgrades of ESXi hosts is a multi-stage process.

1. Populate the vSphere Lifecycle Manager repository with patches, extensions, and updates.
   The vSphere Lifecycle Manager repository contains software updates that you can use with both vSphere Lifecycle Manager baselines and vSphere Lifecycle Manager images. On the **Updates** tab of the vSphere Lifecycle Manager home view, you see all software updates available in the vSphere Lifecycle Manager depot as bulletins.
   Updates get into the vSphere Lifecycle Manager local depot through synchronization with configurable download sources. By default, vSphere Lifecycle Manager is configured to synchronize updates from the official VMware depot.
   You can also import updates into the depot manually.
   For host upgrade operations through baselines, you use ESXi ISO images, which you must also import to the vSphere Lifecycle Manager depot manually.
   For more information about working with the vSphere Lifecycle Manager depot, see Working with the vSphere Lifecycle Manager Depot.
2. Create baselines by combining bulletins from the depot and using manually uploaded ESXi ISO images.
   You can also combine several non-conflicting baselines to create a baseline group. Baseline groups can contain different types of baselines. If a baseline group contains both upgrade and patch or extension baselines, the upgrade runs first.
   For more information about creating baselines and baseline groups, see Creating and Working with Baselines and Baseline Groups.
3. Attach the baselines to individual ESXi hosts or container objects for ESXi hosts.
   For more information, see Attach Baselines and Baseline Groups to Objects.
4. Check the compliance of ESXi hosts against a selected baseline or baseline group.
   You can run a compliance check on an individual ESXi host or a container object.
   For more information about compliance checks against baselines and baseline groups, see Checking Compliance Against vSphere Lifecycle Manager Baselines and Baseline Groups.
5. Review the compliance status of the scanned object.
   For more information about compliance states, see Viewing Compliance Information About ESXi Hosts and Updates.
6. Optionally, you can stage the patches and extensions to ESXi hosts before remediation. Staging is not a mandatory step, it is a step that you can skip.
   For more information about staging updates before remediation, see Staging Patches and Extensions to ESXi Hosts.
7. Remediate the non-compliant objects. After remediation, you can review the compliance status again to make sure that the updates are installed.
   For more information about remediating objects against baselines and baseline groups, see Remediating ESXi Hosts Against vSphere Lifecycle Manager Baselines and Baseline Groups .

Creating and Working with Baselines and Baseline Groups

You use baselines and baseline groups to update the ESXi hosts in your vSphere inventory. The vSphere Lifecycle Manager baselines are three types: predefined baselines, recommendation baselines, or custom baselines, which you create. Depending on their content, baselines can be patch, extension, or upgrade baselines.

When you initiate a compliance check for an ESXi host, you evaluate it against baselines and baseline groups to determine its level of compliance to those baselines or baseline groups.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, the baselines and baseline groups that you create and manage are applicable only to the inventory objects managed by the vCenter Server system where the selected vSphere Lifecycle Manager instance runs.

In the vSphere Client, the baselines and baseline groups are displayed on the **Baselines** tab of the vSphere Lifecycle Manager home view.

Predefined, Recommendation, and Custom Baselines

Predefined baselines

Predefined baselines cannot be edited or deleted, you can only attach or detach them to inventory objects.

On the **Baselines** tab in the vSphere Lifecycle Manager home view, you can see the following predefined baselines.

- Host Security Patches
  The Host Security Patches baseline checks ESXi hosts for compliance with all security patches.
- Critical Host Patches
  The Critical Host Patches baseline checks ESXi hosts for compliance with all critical patches.
- Non-Critical Host Patches
  The Non-Critical Host Patches baseline checks ESXi hosts for compliance with all optional patches.

The Host Security Patches, and Critical Host Patches predefined baselines are attached by default to the vCenter Server instance where vSphere Lifecycle Manager runs.

Recommendation Baselines

Recommendation baselines are predefined baselines that vSAN generates.

You use recommendation baselines to update your vSAN clusters with recommended critical patches, drivers, updates, or the latest supported ESXi host version for vSAN.

These baselines appear by default when you use vSAN clusters with ESXi hosts of version 6.0 Update 2 and later in your vSphere inventory. If your vSphere environment does not contain any vSAN clusters, no recommendation baselines are created.

Recommendation baselines update their content periodically, which requires vSphere Lifecycle Manager to have constant access to the Internet. The vSAN recommendation baselines are typically refreshed every 24 hours.

Recommendation baselines cannot be edited or deleted. You do not attach recommendation baselines to inventory objects in your vSphere environment. You can create a baseline group by combining multiple recommendation baselines, but you cannot add any other type of baseline to that group. Similarly, you cannot add a recommendation baseline to a baseline group that contains upgrade, patch, and extension baselines.

Custom Baselines

Custom baselines are the baselines that you create. You can create custom patch, extension, and upgrade baselines to meet the needs of your specific deployment.

Baseline Groups

You create a baseline group by assembling existing and non-conflicting baselines. Baseline groups allow you to scan and remediate objects against multiple baselines at the same time.

The following are valid combinations of baselines that can make up a baseline group:

- Multiple host patch and extension baselines.
- One upgrade baseline, multiple patch, and extension baselines.

To create, edit, or delete baselines and baseline groups, you must have the **Manage Baseline** privilege. To attach baselines and baseline groups to target inventory objects, you must have the **Attach Baseline** privilege. The privileges must be assigned on the vCenter Server system where vSphere Lifecycle Manager runs.

For more information about managing users, groups, roles, and permissions, see the *vSphere SecurityvSphere Security* documentation.

For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

Creating Baselines in vSphere 7.0 and Later Releases

Because in vSphere 7.0 and later releases the official VMware online depot hosts certified partner content in addition to VMware content, a broader set of OEM bulletins are available in the vSphere Lifecycle Manager depot. As a result, in the **Create Baseline** and **Edit Baseline** wizards, you also see a broader set of OEM bulletins. Some of these bulletins might have dependencies that must be pulled into the baselines that you create, so that the remediation against those baselines is successful. Always consult the KB article for an individual bulletin before you include it in a baseline. The KB article contains information about the bulletin deployment specifics and required dependencies. You must include in the baseline, only bulletins compatible with the hardware on which the host is running. Otherwise, remediation might fail.

Starting with vSphere 7.0, some changes are also introduced in the way VMware content is packaged. As a result, at patch and update releases, you might see additional bulletins on the patch selection page of the **Create Baseline** and **Edit Baseline** wizards. Those bulletins are usually of the Enhancement or BugFix category. When you include those bulletins in a baseline, you might need to also include base ESXi bulletins in that baseline. To ensure successful application of VMware patches and updates, always include the appropriate roll-up bulletin into your baselines. Otherwise, remediation may fail.

Baseline Types by Content

Depending on their content, vSphere Lifecycle Manager baselines can be upgrade, patch, and extension baselines. You use those types of baselines to check the compliance state of target inventory objects and to remediate the non-compliant objects.

Upgrade Baselines

Host upgrade baselines define the version to which you upgrade the hosts in your environment. With vSphere Lifecycle Manager7.0, you can upgrade ESXi hosts from version 6.5 and 6.7 to ESXi7.0. Host upgrades to ESXi 5.x, ESXi 6.5, or ESXi6.7 are not supported.

To create an upgrade baseline, you must first import an ESXi ISO image to the vCenter Server inventory.

Patch Baselines

Patch baselines define a number of patches that must be applied to a given host. Patch baselines can be either dynamic or fixed.

Baseline	Description
Dynamic Patch Baseline	You specify the criteria for patch inclusion in the baseline. Only the patches that meet the criteria are included in the baseline. As the set of available patches in the vSphere Lifecycle Manager depot changes, dynamic baselines are updated as well. You can manually include or exclude patches from the baseline.
Fixed Patch Baseline	You manually select the patches from the total set of patches available in the vSphere Lifecycle Manager depot.

Extension Baselines

Extensions baselines contain additional software modules for ESXi hosts, for example device drivers. This additional software might be VMware software or third-party software. You can install additional modules by using extension baselines, and update the installed modules by using patch baselines.

Extensions are installed on the hosts that do not yet have such software, and patched on the hosts that already have the software installed. All third-party software for ESXi hosts is classified as host extension, although extensions are not restricted to just third-party software.

Create a Fixed Patch Baseline

A fixed baseline is a set of patches that does not change as patch availability in the depot changes.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select **New** > **Baseline**.
   The **Create Baseline** wizard opens.
3. On the **Name and Description** page, enter information about the baseline and click **Next**.
   a) Enter a name and, optionally, a description for the baseline.
   b) Select the **Upgrade**, **Patch**, or **Extension** radio button.
4. On the **Select Patches Automatically** page, stop the automatic updates by deselecting the respective check box and click **Next**.
5. On the **Select Patches Manually** page, select the patches that you want to include in the baseline and click **Next**.
   - To view only the rollup bulletins in the list, turn on the **Show only rollup updates** toggle swtich.
   - To filter the patches that are available in the vSphere Lifecycle Manager depot and find specific patches to include in the baseline, use the filter icon next to each column header. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND.
6. On the **Summary** page, review your selections and click **Finish**.

The new baseline appears in the baselines list on the **Baselines** tab.You can attach the baseline to a data center, a cluster, or a host.

Create a Dynamic Patch Baseline

A dynamic baseline is a set of patches that meet certain criteria. The content of a dynamic baseline changes as the available patches change. You can manually exclude or add specific patches to the baseline.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select **New** > **Baseline**.

   The **Create Baseline** wizard appears.
3. On the **Name and Description** page, enter information about the baseline and click **Next**.
   a) Enter a name and, optionally, a description for the baseline.
   b) Select the **Upgrade**, **Patch**, or **Extension** radio button.
4. On the **Select Patches Automatically** page, set the criteria for adding patches to the baseline.
   a) Enable the automatic update of the baseline by selecting the respective check box.
   b) On the **Criteria** tab, specify the criteria that a patch must meet to be added to the baseline and click **Next**.

      The relationship between these fields is defined by the Boolean operator AND.

      For example, when you select a product and severity option, the patches are restricted to the ones that are applicable for the selected product and are of the specified severity level.
   c) Optional: On the **Matched** tab, deselect patches from the ones that matched your criteria to exclude them permanently from the baseline.
   d) Optional: On the **Excluded** and **Selected** tabs, view the patches that are are excluded from the baseline and the ones that are included in the baseline.

   You can use the filter icon next to each column header on the **Matched**, **Excluded**, and **Selected** tabs to filter the patches that are available in the vSphere Lifecycle Manager depot. This way, you can easily find specific patches to exclude from or include in the baseline. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND.
5. On the **Select Patches Manually** page, select individual patches to include in the baseline and click **Next**.

   The patches that are displayed on this page are patches that do not meet the criteria you set on the **Select Patches Automatically** page. You can use the filter icon next to each column header to filter the patches that are available in the vSphere Lifecycle Manager depot and find specific patches to include in the baseline. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND.

   The patches that you add manually to the dynamic baseline stay in the baseline regardless of the automatically downloaded patches.
6. On the **Summary** page, review your selections and click **Finish**.

The new baseline appears in the baselines list on the **Baselines** tab.You can attach the baseline to a data center, a cluster, or a host.

Create a Host Extension Baseline

Extension baselines contain additional software for ESXi hosts. This additional software might be VMware software or third-party software.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

Extensions deliver additional host features, updated drivers for hardware, Common Information Model (CIM) providers for managing third-party modules on the host, improvements to the performance or usability of the existing host features, and so on.

The host extension baselines that you create are always fixed. You must carefully select the appropriate extensions for the ESXi hosts in your environment.

You use extension baselines to install extensions on the ESXi hosts in your environment. After an extension is installed on a host, you can update the extension module through either patch, or extension baselines.

Note: When you use extension baselines, you must be aware of the functional implications that the installation of new modules on the host might have. Extension modules might alter the behavior of ESXihosts. During the installation of extensions, vSphere Lifecycle Manager only performs the checks and verifications expressed at the package level.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select **New** > **Baseline**.
   The **Create Baseline** wizard appears.
3. On the **Name and Description** page, enter information about the baseline and click **Next**.
   a) Enter a name and, optionally, a description for the baseline.
   b) Select the **Extension** radio button.
4. On the **Select Extensions** page, select individual extensions to include in the baseline and click **Next**.
   You can use the filter icon next to each column header to filter the extensions that are available in the vSphere Lifecycle Manager depot and find specific extensions to include in the baseline. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND.
5. On the **Select Extensions** page, select individual extensions to include in the baseline and click **Next**.
6. On the **Summary** page, review your selections and click **Finish**.

The new baseline appears in the baselines list on the **Baselines** tab.You can attach the baseline to a data center, a cluster, or a host.

Create a Host Upgrade Baseline

You can create upgrade baselines for ESXi hosts with ESXi7.0 images, whichyou must first import to the vSphere Lifecycle Manager depot.

- Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**.
- Verify that you have an ESXi7.0 image available in inventory. For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.

You can use ESXi `.iso` images to upgrade ESXi 6.5.x hosts and ESXi6.7.x hosts to ESXi7.0.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-7.0.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder. You can also use ISO images created and distributed by OEMs.

Note: In case of an unsuccessful upgrade from ESXi 6.5 or ESXi6.7 to ESXi7.0, you cannot roll back to your previous ESXi 6.5 or ESXi6.7 instance.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. Start the **Create Baseline** wizard.
   - On the **Imported ISOs** tab, select an ESXi image from the list and click **New Baseline**.
   - On the **Baselines** tab, select **New** > **Baseline**.
3. On the **Name and Description** page, enter information about the baseline and click **Next**.
   a) Enter a name and, optionally, a description for the baseline.
   b) Select the **Upgrade** radio button.
4. On the **Select ISO** page, select an ESXi image from the list and click **Next**.
5. On the **Summary** page, review your selections and click **Finish**.

The new baseline appears in the baselines list on the **Baselines** tab.You can attach the baseline to a data center, a cluster, or a host.

Create a Host Baseline Group

You can combine multiple baselines of different types into a baseline group. For example, you can combine one host upgrade baseline with multiple patch or extension baselines, or you can combine multiple patch and extension baselines.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

A baseline group might contain a single host upgrade baseline and multiple patch or extension baselines, or a combination of host patch and host extension baselines.
You can create a baseline group and add baselines to it later.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select **New** > **Baseline Group**.

   The **Create Baseline Group** wizard opens.

3. On the **Name and Description** page, enter a unique name and, optionally, a description for the baseline group, and click **Next**.
4. Optional: On the **Upgrade Baseline** page, select an upgrade baseline to include in the baseline group and click **Next** .
   a) Select the **Add the following Upgrade Baseline to the Group** check box.
   b) Select an upgrade baseline from the list.
5. Optional: On the **Patch Baselines** page, select patch baselines to include in the baseline group and click **Next**.
6. Optional: On the **Extension Baselines** page, select extension baselines to include in the baseline group and click **Next**.
7. On the **Summary** page, review your selections and click **Finish**.

The new host baseline group appears in the baselines list on the **Baselines** tab. You can attach the baseline group to a data center, a cluster, or a host.

Edit a Patch Baseline

You can edit existing patch baselines.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select a patch baseline from the list and click **Edit**.

   The **Edit Baseline** wizard appears.
3. Optional: On the **Name and Description** page, edit the name and, optionally, the description of the baseline.
4. Optional: On the **Select Patches Automatically** page, change the criteria for a patch selection and click **Next**.
5. Optional: On the **Select Patches Manually** page, change the selected patches and click **Next**.

   You can deselect patches, or select new ones to include in the patch baseline.
6. On the **Summary** page, review your selections and click **Finish**.

Attach the baseline to a data center, a cluster, or a host.

Edit a Host Extension Baseline

You can change the name, description, and composition of an existing extension baseline.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2. On the **Baselines** tab, select an extension baseline from the list and click **Edit**.
   The **Edit Baseline** wizard appears.
3. Optional: On the **Name and Description** page, edit the name and, optionally, the description of the baseline.
4. Optional: On the **Select Extensions** page, change the included extensions and click **Next**.
5. On the **Summary** page, review your selections and click **Finish**.

Attach the baseline to a data center, a cluster, or a host.

Edit a Host Upgrade Baseline

You can change the name of an existing upgrade baseline. You can also select a different ESXi image for the baseline.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select an upgrade baseline from the list and click **Edit**.
   The **Edit Baseline** wizard appears.
3. Optional: On the **Name and Description** page, edit the name and, optionally, the description of the baseline.
4. Optional: On the **Select ISO** page, change the included ESXi image and click **Next**.
5. On the **Summary** page, review your selections and click **Finish**.

Edit a Baseline Group

You can change the name and type of an existing baseline group. You also use the **Edit Baseline Group** wizard to add or remove baselines to an existing baseline group.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select a baseline group from the list and click **Edit**.
   The **Edit Baseline Group** wizard opens.
3. Optional: On the **Name and Description** page, edit the name, description, or the ESXi version for the baseline group.
4. Optional: On the **Upgrade Baseline** page, select an upgrade baseline and select your task, and click **Next**.
   - To add the selected upgrade baseline to the baseline group, select the **Add the following Upgrade Baseline to the Group** check box.
   - To remove the selected upgrade baseline from the baseline group, deselect the **Add the following Upgrade Baseline to the Group** check box.

5. Optional: On the **Patch Baselines** page, specify which patch baselines are included in the baseline group and click **Next**.
   - To add patch baselines to the baseline group, select the respective patch baselines.
   - To remove patch baselines from the baseline group, deselect the respective patch baselines.
6. Optional: On the **Extension Baselines** page, specify which extension baselines are included in the baseline group and click **Next**.
   - To add extension baselines to the baseline group, select the respective extension baselines.
   - To remove extension baselines from the baseline group, deselect the respective extension baselines.
7. On the **Summary** page, review your selections and click **Finish**.

Attach the baseline group to a data center, a cluster, or a host.

Add or Remove a Single Update from a Custom Baseline

You can edit the content of a custom baseline by adding or removing individual patches or extension from the baseline.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. Click the **Updates** tab.
   You see a list of all updates in the vSphere Lifecycle Manager depot.
3. Select a patch or extension from the list, and click **Add/Remove Baselines**.
   The **Add/Remove baselines** dialog box opens.
4. Select your task.
   - To add the patch to a baseline, select that baseline in the **Custom Patch Baselines** list.
   - To remove the patch from a baseline, deselect that baseline in the **Custom Patch Baselines** list.
5. Click **OK**.

Duplicate Baselines and Baseline Groups

You can duplicate baselines and baseline groups and edit the copies without the risk of compromising the original baseline.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.
      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select a baseline or a baseline group from the list and click **Duplicate**.
   The **Duplicate Baseline** dialog box opens.

3. Enter a name for the new baseline or baseline group or use the suggested one.
4. Click **Duplicate** to confirm the creation of a duplicate copy of the selected baseline or baseline group.

The duplicated baseline or baseline group appears in the **Baselines** list on the **Baselines** tab.

Delete Baselines and Baseline Groups

You can delete the baselines and baseline groups that you no longer need. Deleting a baseline detaches it from all the objects to which it is attached. You cannot delete predefined and system-managed baselines.

Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines**

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Baselines** tab, select a baseline or a baseline group from the list and click **Delete**.

   The **Delete Baseline** dialog box opens.
3. Click **Yes** to confirm the deletion of the selected baseline or baseline group.

Attaching Baselines and Baseline Groups to vSphere Objects

To update ESXi hosts by using vSphere Lifecycle Manager baselines and baseline groups, you must first attach the baselines and baseline groups to individual hosts, clusters, or container objects.

When you no longer need baselines or baseline groups, you can detach them from the objects.

Attach Baselines and Baseline Groups to Objects

To check the compliance status of the objects in your inventory against selected baselines and baseline groups, you must first attach the respective baselines and baseline groups to the objects.

- If you want to attach a baseline or a baseline group to a cluster, verify that the cluster is not configured to use a single image.
- Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines** > **Attach Baseline**.

You attach baselines and baseline groups to individual hosts or objects that contain hosts, such as clusters, data centers, and vCenter Server instances. In the vSphere infrastructure hierarchy, the baseline and baseline groups that you attach to container objects are also attached to the child objects. For example, if you attach a baseline or baseline group to a folder, the baseline or the baseline groups is inherited by all the objects in the folder, including subfolders.

You cannot use vSphere Lifecycle Manager to update the hosts in a cluster that uses a single vSphere Lifecycle Manager image. For more information about using vSphere Lifecycle Manager images to manage hosts in clusters collectively, see Using vSphere Lifecycle Manager Images .

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines**.
3. In the **Attached Baselines** pane, click **Attach** > **Attach Baseline or Baseline Group**.
   The **Attach** dialog box opens.
4. Select one or more baselines or baseline groups and click **Attach**.
   If you select a baseline group, all the baselines in it are attached to the object.
   The selected baselines or baseline groups are attached to the object. They appear on the list in the **Attached Baselines** pane. If the selected object is a container object, the selected baselines or baseline groups are attached to all the child objects.

Scan the selected object against the attached baselines.

Detach Baselines and Baseline Groups from Objects

You can detach baselines and baseline groups from the objects to which the baselines or baseline groups are directly attached.

- Verify that the cluster is not configured to manage all its hosts collectively.
- Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Baselines** > **Attach Baseline**.

vSphere inventory objects might have inherited properties, so instead of detaching baselines and baseline groups directly from an object, you might need to select its container object and detach the baselines or baseline groups from the container object. For example, if you want to detach a baseline or a baseline group from a host that is a part of a cluster, you must select the cluster and not the host.

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines**.
3. In the **Attached Baselines** pane, select one or more baselines or baseline groups and click **Detach**.
   The **Detach** dialog box opens.
4. Select the object to detach the baseline or baseline group from and click **Detach**.
   The baseline is removed from the **Attached Baselines** list.

Checking Compliance Against vSphere Lifecycle Manager Baselines and Baseline Groups

Before you update or upgrade an ESXi host or a container object with vSphere Lifecycle Manager baselines, you must first check its compliance status.

You use vSphere Lifecycle Manager to check the compliance status of ESXi hosts against the baselines and baseline groups that you attach to the hosts or to a parent container object. You do a compliance check on hosts to determine

whether they have the latest patches or extensions. During the compliance check, attributes of the host are evaluated against all patches, extensions, and upgrades from an attached baseline or baseline group.

You can check the compliance status of a single ESXi host or a valid container object. Supported groups of ESXi hosts include virtual infrastructure container objects such as folders, clusters, and data centers. When you initiate a compliance check for a container object, vSphere Lifecycle Manager scans all the ESXi hosts in that container object.

Note: If you initiate a compliance check for an inventory object, for example data center, that contains clusters that use vSphere Lifecycle Manager images, the compliance check is not performed for those clusters. Operations

To generate compliance information, you can initiate compliance checks manually or you can schedule the compliance checks to run at regular periods. Schedule compliance checks at a data center or vCenter Server system level to make sure that the objects in your inventory are up-to-date.

You check the compliance status of vSphere objects from the vSphere Lifecycle Manager compliance view.

To initiate or schedule compliance checks, you must have the **Scan for Applicable Patches, Extensions, and Upgrades** privilege.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

Initiate a Compliance Check for ESXi Hosts Manually

Before remediation, you must check the compliance of the vSphere objects against the attached baselines and baseline groups. To check the compliance status of hosts in the vSphere inventory immediately, initiate a compliance check manually.

If you want to check the compliance status of a cluster, verify that the cluster is not configured to use a single image.

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines**.
   The **Baselines** pane shows three panels. In those panels, you obtain host information about the selected object, host compliance information, and remediation information.
3. In the compliance information panel, click **Check Compliance**.

The selected inventory object and all child objects are scanned against all attached patch, extension, and upgrade baselines. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes.

Schedule Regular Compliance Checks for ESXi Hosts

You can configure vSphere Lifecycle Manager to check the compliance status of ESXi hosts at specific times or at intervals that are convenient for you.

If you want to check the compliance status of a cluster, verify that the cluster is not configured to use a single image.

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines**.
   The **Baselines** pane shows three panels. In those panels, you obtain host information about the selected object, host compliance information, and remediation information.
3. In the compliance information panel, click **Schedule**.
   The **Automatic compliance check** dialog box opens.
4. Configure the compliance check schedule.
   a) Set the frequency and the starting point of the compliance check.
   b) Enter a unique name, and optionally, a description for the scan task.
   c) Optional: Specify one or more email addresses to receive notification after the scan task is complete.
      You must configure mail settings for the vCenter Server system to enable this option.
5. Click **Save** to exit the **Automatic compliance check** dialog box.

Host Upgrade Compliance Messages

When you check the compliance of ESXi hosts against an upgrade baseline, vSphere Lifecycle Manager runs a precheck script and provides informative messages in the in the bottom pane of the vSphere Lifecycle Manager compliance view. The messages notify you about potential problems with hardware or third-party software on the host, and configuration issues, which might prevent a successful upgrade to ESXi7.0.

The messages that vSphere Lifecycle Manager provides correspond to error or warning codes from running the host upgrade precheck script.

For interactive installations and upgrades performed by using the ESXi installer, the errors or warnings from the precheck script are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations and upgrades, the errors or warnings are written to the installation log.

vSphere Lifecycle Manager displays scan result information in the bottom pane of the vSphere Lifecycle Manager compliance view. To see the original errors and warnings returned by the precheck script during an vSphere Lifecycle Manager host upgrade scan operation, review the vSphere Lifecycle Manager log file.

Table 121: Scan Result Messages and Corresponding Error and Warning Codes

Scan Result Message in vSphere Lifecycle Manager	Description
`Host CPU is unsupported. New ESXi version requires a 64-bit CPU with support for LAHF/SAHF instructions in long mode.`	This message appears if the host processor is 32-bit and does not support required features. The corresponding error code is `64BIT_LONGMODESTATUS`.
`Trusted boot is enabled on the host but the upgrade does not contain the software package esx-tboot. Upgrading the host will remove the trusted boot feature.`	This message indicates that the host upgrade scan did not locate the `esx-tboot` VIB on the upgrade ISO. The corresponding error code is `TBOOT_REQUIRED`

Scan Result Message in vSphere Lifecycle Manager	Description
VMkernel and Service Console network interfaces are sharing the same subnet *subnet_name*. This configuration is not supported after upgrade. Only one interface should connect to subnet *subnet_name*.	Warning. An IPv4 address was found on an enabled Service Console virtual NIC for which there is no corresponding address in the same subnet in the vmkernel. A separate warning appears for each such occurrence. The corresponding error code is COS_NETWORKING.
New ESXi version requires a minimum of *core_count* processor cores.	The host must have at least two cores. The corresponding error code is CPU_CORES.
Processor does not support hardware virtualization or it is disabled in BIOS. Virtual machine performance may be slow.	Host performance might be impaired if the host processor does not support hardware virtualization or if hardware virtualization is not turned on in the host BIOS. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation. The corresponding error code is HARDWARE_VIRTUALIZATION.
Insufficient memory, minimum *size_in_MB* required for upgrade.	The host requires the specified amount of memory to upgrade. The corresponding error code is MEMORY_SIZE.
Host upgrade validity checks for *file_name* are not successful.	This test checks whether the precheck script itself can be run. The corresponding error code is PRECHECK_INITIALIZE.
The host partition layout is not suitable for upgrade.	Upgrade is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition starts after sector 1843200. The corresponding error code is PARTITION_LAYOUT.
Unsupported configuration.	The file /etc/vmware/esx.conf must exist on the host. This message indicates that the file /etc/vmware/esx.conf is either missing, or the file data cannot be retrieved or read correctly. The corresponding error code is SANE_ESX_CONF.
The host does not have sufficient free space on a local VMFS datastore to back up current host configuration. A minimum of *size_in_MB* is required.	The host disk must have enough free space to store the ESXi 5.x configuration between reboots. The corresponding error code is SPACE_AVAIL_CONFIG.
The upgrade is not supported for current host version.	Upgrading to ESXi7.0 is possible only from ESXi 6.5 and ESXi6.7 hosts. The corresponding error code is SUPPORTED_ESX_VERSION.
Unsupported devices *device_name* found on the host.	The script checks for unsupported devices. Some PCI devices are not supported with ESXi7.0. The corresponding error code is UNSUPPORTED_DEVICES.
Host software configuration requires a reboot. Reboot the host and try upgrade again.	To ensure a good bootbank for the upgrade, you must reboot the hosts before remediation. The corresponding error code is UPDATE_PENDING.
In an environment with Cisco Nexus 1000V Distributed Virtual Switch, vSphere Lifecycle Manager displays different messages in different situations. For details, see Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present.	If Cisco's Virtual Ethernet Module (VEM) software is found on the host, the precheck script checks if the software is part of the upgrade as well, and that the VEM supports the same version of the Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the script returns a warning and the scan result indicates the version of the VEM software that was expected on the upgrade ISO, and the version, if any, that was found on the ISO.

Scan Result Message in vSphere Lifecycle Manager	Description
	The corresponding error code is `DISTRIBUTED_VIRTUAL_SWITCH`.
`The host uses an EMC PowerPath multipathing module` *`file_name`* `to access storage. The host will not be able to access such storage after upgrade.`	The script checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the script verifies that matching components (CIM, VMkernel module) also exist in the upgrade. If they do not, the script returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found. The corresponding error code is `POWERPATH`.

Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present

When a host is managed by the Cisco Nexus 1000V virtual switch and you check the compliance of the host against an upgrade baseline, the scan messages provide information about problems with compliance between the VEM modules installed on the host and the modules available on the ESXi7.0 image.

vSphere Lifecycle Manager supports Cisco Nexus 1000V, a virtual access software switch that works with VMware vSphere and consists of two components.

Virtual Supervisor Module (VSM)	The control plane of the switch and a virtual machine that runs NX-OS.
Virtual Ethernet Module (VEM)	A virtual line card embedded in ESXi hosts.

vSphere Lifecycle Manager determines whether a host is managed by Cisco Nexus 1000V. vSphere Lifecycle Manager verifies whether the Cisco Nexus 1000V VEM VIBs in the ESXi upgrade image are compatible with the Cisco Nexus 1000V VSM that manages the host.

By using vSphere ESXi Image Builder, you can create custom ESXi images, which contain third-party VIBs that are required for a successful remediation operation.

Table 122: Compliance Check Results for the Cisco Nexus 1000V Network Switch

Compliance Check Message	Description
`The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V software package on the host. Upgrading the host will remove the feature from the host.`	A VEM VIB is not available on the ESXi7.0 upgrade image.
`The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade contains a Cisco Nexus 1000V software package` *`VIB_name`* `that is incompatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.`	The VEM VIB on the ESXi7.0 upgrade image is not compatible with the version of the VSM.
`The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.`	The host and the image do not contain VEM VIBs, but the host is still listed in vCenter Server as managed by Cisco Nexus 1000V.

Compliance Check Message	Description
`Cannot determine whether the upgrade breaks Cisco Nexus 1000V virtual network switch feature on the host. If the host does not have the feature, you can ignore this warning.`	There was a problem with determining compatibility between the VEM VIB on the ESXi7.0 upgrade image and the VSM. Check whether the version of the VSM managing the host is certified as being compatible with vCenter Server7.0 and ESXi7.0.

Viewing Compliance Information About ESXi Hosts and Updates

vSphere Lifecycle Manager scans objects to determine how they comply with the baselines and baseline groups that you attach to those objects. You can view compliance information about a single ESXi host or a group of hosts in a container object.

Supported groups of ESXi hosts include virtual infrastructure container objects such as folders, clusters, and data centers.

The host or the container object must have an attached baseline or baseline group to be examined for compliance information. Compliance with baselines and baseline groups is assessed at the time of viewing.

The overall compliance status of an ESXi hosts depends on the compliance statuses of all baselines and baseline groups that are attached to the object. For information about the different compliance statuses that an object, a baseline or a baseline group might have, see Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups .

The compliance status of a baseline depends on the compliance statuses of all updates in the baseline. For information about the compliance statuses that updates might have, see Compliance Statuses of Updates.

The ability to view the compliance status of vSphere objects depends on the privileges that you have. To view the compliance status of an inventory object, you must have the **View Compliance Status** privilege. Users that have privileges to remediate against patches, extensions, and upgrades and to stage patches and extensions on a particular inventory object, can view the compliance status of the same object even if they do not have the **View Compliance Status** privilege.

- Users with the privilege to view a container, but not all the contents of the container, can view the aggregate compliance status of all objects in the container.
- If a user does not have the permission to view an object, its contents, or a particular virtual machine, the results of those scans are not displayed.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

For information about checking the compliance of hosts against an image, see Check Cluster Compliance Against an Image.

The vSphere Lifecycle Manager Compliance View

Compliance information about inventory objects is displayed on the **Updates** tab for the object, in the so-called vSphere Lifecycle Manager compliance view.

The vSphere Lifecycle Manager compliance view for objects that you manage with baselines and baseline groups consists of three panes.

Table 123: vSphere Lifecycle Manager Compliance View

Pane	Description
Baselines	The **Baselines** pane has three information panels. • Host Information panel For individual ESXi hosts, this panel shows information about the ESXi version installed on the host. You can also view all updates that are installed on the host. For container objects, this panel shows information about the ESXi versions of all hosts in the container object. • Compliance Information panel For individual ESXi hosts, this panel shows the overall compliance status of the host against all attached baselines and baseline groups. You can also view compliance information about the baselines and baseline groups attached to the host. For container objects, this panel shows the overall number of compliant and non-compliant hosts. This panel also shows the last time a compliance check was completed. • Remediation Information panel This panel shows the result of the remediation pre-check and indicates whether the selected object is ready for remediation. The panel also contains information about the issues that require user attention or action. This panel also shows the last time a remediation pre-check was completed. The information in the **Baselines** pane changes dynamically depending on the inventory object, baselines, and baseline groups that you select.
Attached Baselines and Baseline Groups	Displays the baselines and baseline groups attached to the selected object.
Bottom pane	The bottom pane appears when you select a baseline or a baseline group from the **Attached Baselines and Baseline Groups** pane. The information in this pane depends on the type of inventory object that you select. For individual hosts, the bottom pane shows information about all updates in the baseline or baseline group that you select from the **Attached Baselines and Baseline Groups** pane. • If you select a patch baseline or extension baseline, the bottom pane shows a list of all updates that the selected baseline contains. • If you select an upgrade baseline, the bottom pane shows information about the ESXi image that the upgrade baseline contains. • If you select a baseline group, the bottom pane shows all baselines included in the group along with their compliance statuses. You can also view all the updates that the baseline group contains. If the baseline group contains an ESXi image, information about it is also displayed in the bottom pane. For container objects, the bottom pane displays compliance information about the ESXi hosts that have the selected baseline or baseline group. When you select a baseline or a baseline group from the **Attached Baselines and Baseline Groups** pane, the bottom pane appears and displays all the hosts to which the selected baseline or baseline group is attached along with the individual compliance statuses of those hosts.

Compliance Statuses of Updates

When you work with vSphere Lifecycle Manager baselines, an update stands for all patches, extensions, and upgrades that you can apply with vSphere Lifecycle Manager baselines. The compliance status of the updates in the baselines and

baseline groups that you attach to objects in your inventory is calculated after you check the compliance of the target object.

The compliance statuses of the updates in a baseline define the overall compliance status of that baseline. For more information about baseline compliance statuses, see Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups .

Conflict	The update conflicts with either an existing update on the host or another update in the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform compliance checks, remediation, and staging operations. In most cases, you must resolve the conflict.
Conflicting New Module	The host update is a new module that provides software for the first time, but it is in conflict with either an existing update on the host or another update in the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you must resolve the conflict.
Incompatible Hardware	The hardware of the selected object is incompatible or has insufficient resources to support the update. For example, when you perform a host upgrade scan against a 32-bit host or if a host has insufficient RAM.
Installed	The update is installed on the target object and no further user action is required.
Missing	The update is applicable to the target object, but it is not yet installed. You must perform a remediation on the target object with this update, so that the update becomes compliant.
Missing Package	The metadata for the update is in the depot, but the corresponding binary payload is missing. The reasons can be that the product might not have an update for a given locale; the vSphere Lifecycle Manager depot is corrupt, and vSphere Lifecycle Manager no longer has Internet access to download updates; or you have manually deleted an upgrade package from the vSphere Lifecycle Manager depot.
New Module	The update is a new module. An update with this compliance status cannot be installed when it is part of a host patch baseline. When it is part of a host extension baseline, the new module status indicates that the module is missing on the host and can be provisioned by remediation. The compliance status of the baseline depends on the type of baseline containing the update with the New Module status. If the baseline is a host patch baseline, the overall status of the baseline is compliant. If the baseline is a host extension baseline, the overall status of the baseline is non-compliant.
Not Applicable	The update is not applicable to the target object. A patch might have the not applicable compliance status for one of the following reasons: • There are other patches in the vSphere Lifecycle Manager depot that obsolete this patch.

	• The update does not apply to the target object.
Not Installable	The update cannot be installed. The compliance check might succeed, but the remediation of the target object cannot be performed.
Obsoleted By Host	This compliance status is mainly applicable to patches. The target object has a newer version of the patch. For example, if a patch has multiple versions, after you apply the latest version to the host, the earlier versions of the patch have the Obsoleted By Host compliance status.
Staged	This compliance status applies to host patches and host extensions. It indicates that the update is copied from the vSphere Lifecycle Manager depot to the host, but it is not yet installed. Staged compliance status might occur only when you check the compliance status of hosts running ESXi 6.5 and later.
Unknown	A patch is in the unknown state for a target object until vSphere Lifecycle Manager successfully scans the object. A scan might not succeed if the target object is of an unsupported version, if vSphere Lifecycle Manager lacks metadata, or if the patch metadata is corrupt.
Unsupported Upgrade	The upgrade path is not supported. For example, the current hardware version of the virtual machine is later than the latest version supported by the host.

Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups

Compliance statuses are computed after you initiate a compliance check for an inventory object against the attached baselines or baseline groups. The compliance statuses that baselines and baseline groups might have depend on the applicability of the patches, extensions, and upgrades contained in the baseline or baseline group attached to an object. The compliance status of a single host depends on the compliance statuses of all baselines and baseline groups attached to the host.

Compliant

The compliant status indicates that a vSphere object is compliant with all baselines in an attached baseline group or with all patches, extensions, and upgrades in an attached baseline. The compliant state requires no further action. If a baseline contains patches or upgrades that are not relevant to the target object, the individual updates, and baselines or baseline groups that contain them, are treated as not applicable, and represented as compliant. Compliant are also hosts with attached patch baselines containing extensions or patches with the obsoleted by host status.

The compliant status occurs under the following conditions:

- Target objects are compliant with the baselines and baseline groups when all updates in the baseline or baseline group are either installed on the target object, obsoleted by host, or are not applicable to the target object.
- The updates in a baseline are compliant when they are installed on the target object, or are not applicable to the object.

Non-Compliant

The non-compliant status indicates that one or more baselines in a baseline group, or one or more patches, extensions, or upgrades in a baseline are applicable to the target object, but are not installed (missing) on the target. You must remediate the target object to make it compliant.

When a baseline contains a non-compliant update, the overall status of the baseline is non-compliant. When a baseline group contains a non-compliant baseline, the overall status of the baseline group is non-compliant. The non-compliant status takes precedence over the incompatible, unknown, and compliant states.

Unknown

When you attach a baseline or a baseline group to a vSphere object and you do not initiate a compliance check for the object, the status of the vSphere object against the baseline or baseline group is unknown. This status indicates that a compliance check is required, that the compliance check has failed, or that you initiated a compliance check on an unsupported platform.

When a baseline contains updates in the compliant and unknown states, the overall status of the baseline is unknown. When a baseline group contains unknown baselines and compliant baselines, the overall status of the baseline group is unknown. The unknown compliance status takes precedence over the compliant status.

Incompatible

The incompatible status requires attention and further action. You must determine the reason for incompatibility by probing further. You can remediate the objects that have this status, but the operation might not be successful. In most cases, vSphere Lifecycle Manager provides sufficient details for the incompatibility.

When a baseline contains updates in the incompatible, compliant, and unknown states, the overall status of the baseline is incompatible. When a baseline group contains incompatible, unknown, and compliant baselines, the overall status of the baseline group is incompatible. The incompatible compliance status takes precedence over the compliant and unknown compliance statuses.

View Compliance Information About ESXi Hosts

You can check how the ESXi hosts in your environment comply with the baselines and baseline groups that you attach to those hosts. You can check and view the compliance status of an individual host or a container object.

- Verify that the host for which you want to view compliance information uses baselines and is not managed with a single vSphere Lifecycle Manager image.
- Review the The vSphere Lifecycle Manager Compliance View topic.

Compliance checks provide information about the degree of compliance of an object with the attached baselines and baseline groups.

In the compliance view for an object, you can view information about the compliance of the object with the attached baselines and baselines groups. You can also view the individual compliance statuses of the attached baselines and baseline groups. The compliance view changes dynamically and depends on the object that you want to view compliance information about. For a full description of the compliance information that you can obtain about an object, seeThe vSphere Lifecycle Manager Compliance View.

For information about the different compliance statuses that an object might have, see Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups .

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines** and review the compliance information in the compliance view.

You see complete compliance information about the selected object.

View Information About the Patches, Extensions, and ISO Images in a Baseline

You can view information about the patches, extensions, and upgrades included in a baseline or a baseline group.

- Verify that the host for which you want to view compliance information uses baselines and is not managed with a single vSphere Lifecycle Manager image.
- Review the The vSphere Lifecycle Manager Compliance View topic.

For information about the different compliance statuses that an update might have, see Compliance Statuses of Updates.

1. In the vSphere Client, navigate to a single ESXi host, cluster, or a valid container object.
2. On the **Updates** tab, select **Hosts** > **Baselines**.
3. In the **Attached Baselines and Baseline Groups** pane, select a baseline.

   A new pane appears below the **Attached Baselines and Baseline Groups** pane. Depending on the selected object, the bottom pane might contain information about the updates and ESXi images in the baseline that you select. If the selected object is a container for ESXi hosts, the bottom pane shows the compliance of each ESXi in the container object against the selected baseline.

Baseline Type	Available Information
Patch	The bottom pane contains a table that lists all patches in the baseline. For each update, you can see the following information. • **Update Name** • **Update ID** The update ID is a vendor-assigned identification code of the patch. • **Status** The **Status** column shows the compliance status of the update. • **Severity** • **Category** • **Impact** The **Impact** column displays the actions that you must take to install the update. For example, rebooting the system or putting the host in maintenance mode. • **ESXi Version**
Upgrade	The bottom pane displays the following information. • **ESXi Version** • **Build** • **Status** The **Status** column shows the compliance status of the update. • **Release Date** • **Vendor** • **Details** • **Release Notes**

Baseline Type	Available Information
	• **Acceptance Level** ESXi images can be either Signed or Unsigned, which indicates their level of acceptance by VMware. The software packages included in ESXi images might have any of the following acceptance levels. **VMware Certified** — The package has gone through a rigorous certification program that verifies the functionality of the feature, and is signed by VMware with a private key. VMware provides customer support for these packages. **VMware Accepted** — The package has gone through a less rigorous acceptance test program that only verifies that the package does not destabilize the system, and is signed by VMware with a private key. The test regimen does not validate the proper functioning of the feature. VMware support hands off support calls directly to the partner. **Partner Supported** — The partner has signed an agreement with VMware and has demonstrated a sound test methodology. VMware provides a signed private/public key pair to the partner to use for self-signing their packages. The VMware support team redirects support calls directly to the partner. **Community Supported** — The package is either unsigned or signed by a key that is not cross-signed by VMware. VMware does not provide support for the package. For support, customers must either use the community or contact the author of the package.
Extension	• **Update Name** • **Update ID** The update ID is a vendor-assigned identification code of the extension. • **Status** The **Status** column shows the compliance status of the update. • **Severity** • **Category**

Baseline Type	Available Information
	• **Impact** The **Impact** column displays the actions that you must take to install the update. For example, rebooting the system or putting the host in maintenance mode. • **ESXi Version**
Baseline Group	To view information about the patches, extension, and ISO images in a baseline group, select the respective tab in the bottom pane. • Click **Baselines** for information about the baselines that a baseline group contains. • Click **ISO** for information about the ESXi image that a baseline group contains. • Click **Updates** for information about the patches and extensions that the baseline group contains.

Staging Patches and Extensions to ESXi Hosts

Staging lets you download the patches and extensions from the vSphere Lifecycle Manager repository to ESXi hosts, without applying the patches and extensions immediately. Staging patches and extensions speeds up the remediation process, because the patches and extensions are already available locally on the hosts.

To stage patches or extensions to hosts, first attach a patch or extension baseline or a baseline group containing patches and extensions to the host. Staging patches and extensions does not require that hosts enter maintenance mode.

With the vSphere Client, you can stage a single baseline, multiple baselines, or baseline groups to a single host or a group of hosts in a container object.

Some limitations exist depending on the compliance status of the patches or extensions that you want to stage.

Patches cannot be staged if they are obsoleted by other patches in the baselines or baseline groups for the same stage operation. vSphere Lifecycle Manager stages only the patches that it can install in a subsequent remediation process, based on the current compliance status of the host. If a patch is obsoleted by patches in the same selected patch set, the obsoleted patch is not staged.

If a patch is in conflict with the patches in the vSphere Lifecycle Manager depot and is not in conflict with a host, after a compliance check, vSphere Lifecycle Manager reports this patch as a conflicting one. You can still stage the patch to the host and after the stage operation, vSphere Lifecycle Manager reports this patch as staged.

During the stage operation, vSphere Lifecycle Manager performs prescan and postscan operations and updates the compliance status of the baseline.

For more information about the different compliance statuses that an update might have, see Compliance Statuses of Updates.

After you stage patches or extensions to hosts, you must remediate the hosts against all staged patches or extensions.

After remediation finishes, the host deletes all staged patches or extensions from its cache regardless of whether they were applied during the remediation. The compliance status of the patches or extensions that were staged but not applied to the hosts reverts from Staged to its previous value.

Important: Staging patches and extensions is supported for hosts that are running ESXi 6.5 and later. You can stage patches to PXE booted ESXi hosts, but if the host is restarted before remediation, the staged patches are lost and you must stage them again.

Stage Patches and Extensions to ESXi Hosts

Staging is the process during which vSphere Lifecycle Manager downloads patches and extensions on the ESXi hosts. During staging, the patches and extensions are not installed on the host. Staging reduces the time that the host spends in maintenance mode during remediation.

- Attach a patch or extension baseline or a baseline group containing patches and extensions to the host.
- Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Patches and Upgrades** > **Stage Patches and Extensions**.

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines**.
3. In the **Attached Baselines** pane, select one or more baselines.
4. Click **Stage**.
   The **Stage Patches** dialog box opens.
5. Select hosts on which to stage patches and extensions.
   The number of selected hosts is on the top of the list.
6. To view the patches or extensions that will download to the selected hosts, expand the **Stage** list.
7. Click **Stage**.

The staging operation starts. You can monitor the progress of the task in the **Recent Tasks** pane.

Remediate the host or hosts.

After remediation, all staged patches and extensions, whether installed or not during the remediation, are deleted from the host.

Remediating ESXi Hosts Against vSphere Lifecycle Manager Baselines and Baseline Groups

Remediation is the process during which vSphere Lifecycle Manager applies patches, extensions, and upgrades to ESXi hosts. Remediation makes the selected vSphere objects compliant with the attached baselines and baseline groups.

General Considerations

- vSphere Lifecycle Manager supports the remediation of ESXi hosts against patch, extension, and upgrade baselines.
- You can initiate remediation manually or schedule a regular remediation task to run at a time that is convenient for you.
- You can remediate a single ESXi host or multiple hosts in a container object. You can initiate remediation at a folder, a cluster, a data center, and even vCenter Server level.
  Note: If you initiate remediation against a baseline for an object that contains clusters that use a single vSphere Lifecycle Manager image, remediation is not performed on those clusters.
- By default, the remediation process runs sequentially. That is, vSphere Lifecycle Manager remediates the hosts in a cluster or another container object one by one. However, you can configure vSphere Lifecycle Manager to remediate multiple hosts in parallel.
- If a vCenter Server instance is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can remediate only the inventory objects managed by the vCenter Server system where the vSphere Lifecycle Manager instance that you use runs.

- To remediate vSphere objects against baselines or baseline groups, you must have the **Remediate to Apply Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.
  For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.
- If a vCenter HA failover is initiated during the remediation of a cluster, the remediation task is canceled. After the failover finishes, you must restart the remediation task on the new node.

Orchestrated Upgrades of ESXi Hosts

You can use baseline groups to perform an orchestrated upgrade of the ESXi hosts in your environment. The baseline group might contain a single host upgrade baseline and multiple patch or extension baselines, or multiple patch and extension baselines. vSphere Lifecycle Manager first upgrades the hosts and then applies the patch or extension baselines. Because the upgrade runs first and patches are applicable to a specific host version, the orchestrated workflow ensures that no patches are lost during the upgrade.

Orchestrated upgrades can be performed at a host, cluster, folder, or a data center level.

Instead of creating a baseline group, you can select and work with multiple baselines instead of grouping them into a baseline group first.

Maintenance Mode

If the update requires it, vSphere Lifecycle Manager puts hosts into maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience, vCenter Server migrates the virtual machines to other hosts within the cluster before the host is put in maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for vMotion and if VMware Distributed Resource Scheduler (DRS) and VMware Enhanced vMotion Compatibility (EVC) are enabled. However, EVC is not a prerequisite for vMotion. EVC guarantees that the CPUs of the hosts are compatible. For container objects or individual hosts that are not in a cluster, migration with vMotion cannot be performed. After remediation, hosts exit maintenance mode. In case of failure during remediation, hosts might be unable to exit maintenance mode.

Parallel Remediation

You can enable vSphere Lifecycle Manager to remediate in parallel the hosts within a cluster that uses baselines. Parallel remediation reduces the time needed for patching or upgrading the hosts in your environment. You can remediate in parallel only ESXi hosts that are already in maintenance mode. During parallel remediation, hosts do not enter maintenance mode automatically. Similarly, after remediation finishes, the hosts do not exit maintenance mode automatically. To remediate hosts in parallel, you must manually enter and exit maintenance mode. If you enable parallel remediation, vSphere Lifecycle Manager does not remediate the ESXi hosts that are not in maintenance mode.

When you configure vSphere Lifecycle Manager to remediate hosts in parallel, you can set the maximum number of hosts to be remediated in a single remediation task. Alternatively, you can let vSphere Lifecycle Manager to remediate all hosts in maintenance mode in parallel.

When you remediate hosts in parallel, if the remediation of a single host fails, the remediation task for the entire cluster does not stop and the rest of the hosts are remediated successfully. After remediation finishes, vSphere Lifecycle Manager reports an error for the respective host.

Parallel remediation is deactivated by default, but you can enable it during remediation or in the vSphere Lifecycle Manager general remediation settings.

You cannot remediate in parallel hosts in a vSAN cluster.

Remediation Pre-Check

Before you remediate an object, you can perform a remediation pre-check on the object. During that check, vSphere Lifecycle Manager identifies possible issues that might prevent successful remediation and takes or suggests actions to fix the issues.

For more information about the possible issues that might prevent successful remediation, see Remediation Pre-Check Report.

Remediation of PXE Booted ESXi Hosts

vSphere Lifecycle Manager lets you remediate PXE booted ESXi hosts. vSphere Lifecycle Manager does not apply the patches that require a reboot to PXE booted ESXi hosts.

If there is any additional software installed on the PXE booted ESXi host, the software might be lost if the host restarts. Update your image profile with the additional software so that it will be present after the reboot.

To patch PXE booted ESXi hosts, you must enable the respective setting in the **Edit Settings for Host Remediation** dialog box, which you open from the **Settings** tab in the vSphere Lifecycle Manager home view.

Understanding the Remediation Operation

For ESXi hosts, updates are all-inclusive. The most recent update contains the patches from all previous releases.

The ESXi image on the host maintains two copies. The first copy is in the active boot and the second one is in the standby boot. When you patch an ESXi host, vSphere Lifecycle Manager creates an image based on the content of the active boot and the content of the patch. The new ESXi image is then located in the standby boot and vSphere Lifecycle Manager designates the active boot as the standby boot and reboots the host. When the ESXi host reboots, the active boot contains the patched image and the standby boot contains the previous version of the ESXi host image.

When you upgrade an ESXi host, vSphere Lifecycle Manager replaces the backup image of the host with the new image and replaces the active boot and the standby boot. During the upgrade, the layout of the disk that hosts the boots changes. The total disk space for an ESXi host remains 1GB, but the disk partition layout within that 1GB disk space changes to accommodate the new size of the boots where the ESXi7.0 image is stored.

For rollback purposes, the term update refers to all ESXi patches, updates, and upgrades. Each time you update an ESXi host, a copy of the previous ESXi build is saved on your host.

If an update fails and the ESXi7.0 host cannot boot from the new build, the host reverts to booting from the original boot build. ESXi permits only one level of rollback. Only one previous build can be saved at a time. In effect, each ESXi7.0 host stores up to two builds, one boot build and one standby build.

The remediation of ESXi 6.5 and 6.7 hosts to their respective ESXi update releases is a patching process, while the remediation of ESXi hosts from version 6.5 or 6.7 to 7.0 is an upgrade process.

From the vSphere Lifecycle Manager settings, you can configure the host remediation process to skip a host reboot during host patch and host upgrade operations. This configuration setting is called Quick Boot. For more information about configuring the vSphere Lifecycle Manager remediation settings, see Configuring the vSphere Lifecycle Manager Remediation Settings.

Types of Host Remediation

Host remediation runs in different ways depending on the types of baselines that you attach to an object and whether the remediated host is in a cluster or not.

Host Upgrade Remediation

When you upgrade an ESXi 6.5 or ESXi6.7 host to ESXi7.0, all supported custom VIBs remain intact on the host after the upgrade, regardless of whether the VIBs are included in the installer ISO.

You can upgrade hosts by using custom ESXi images that contain third-party modules for ESXi7.0. In such a case, third-party modules that are compatible with ESXi7.0 stay available on the upgraded host.

Host upgrade in a high-latency network in which vSphere Lifecycle Manager and the hosts are at different locations might take a few hours because the upgrade file is copied from the vSphere Lifecycle Manager depot to the host before the upgrade. During this time, the host stays in maintenance mode.

vSphere Lifecycle Manager7.0 supports upgrade from ESXi 6.5 and ESXi6.7 to ESXi7.0.

Upgrading to ESXi7.0 requires a boot device that is a minimum of 4 GB. When booting from a local disk, SAN or iSCSI LUN, up to 128 GB of disk space is used to create ESXi system partitions. You can create a VMFS datastore on a boot disk larger than 128 GB.

Note: After you upgrade your host to ESXi7.0, you cannot roll back to the previous ESXi versions, ESXi 6.5, ESXi6.7. So, back up your host configuration before performing an upgrade. If the upgrade fails, you can reinstall the ESXi 6.5 or ESXi6.7 software that you upgraded from and restore your host configuration. For more information about backing up and restoring your ESXi configuration, see the *VMware ESXi Upgrade* documentation. To upgrade ESXi hosts, you must first import ESXi ISO images to the vSphere Lifecycle Manager depot. You then create baselines and baseline groups to manage the upgrades for the ESXi hosts.

Host Patch Remediation

Patching is the process of remediating ESXi hosts against patch baselines.

The remediation of ESXi 6.5 and 6.7 hosts to their respective ESXi update releases is a patching process, while the remediation of ESXi hosts from version 6.5 or 6.7 to 7.0 is an upgrade process.

vSphere Lifecycle Manager handles host patches in the following ways:

- If a patch in a patch baseline requires the installation of another patch, vSphere Lifecycle Manager detects the prerequisite in thedepot and installs it together with the selected patch.
- If a patch is in a conflict with other patches that are installed on the host, the conflicting patch might not be staged or installed. However, if another patch in the baseline resolves the conflicts, the conflicting patch is installed. For example, consider a baseline that contains patch A and patch C, and patch A conflicts with patch B, which is already installed on the host. If patch C obsoletes patch B, and patch C is not in a conflict with patch A, the remediation process installs patches A and C.
- If a patch is in a conflict with the patches in the vSphere Lifecycle Manager depot and is not in a conflict with the host, after a compliance check, vSphere Lifecycle Manager reports this patch as a conflicting one. You can stage and apply the patch to the host.
- When multiple versions of the same patch are selected, vSphere Lifecycle Manager installs the latest version and skips installing the earlier versions.

During patch remediation, vSphere Lifecycle Manager automatically installs the prerequisites of the patches.

With vSphere Lifecycle Manager7.0, you can remediate hosts of version ESXi 6.5 and ESXi6.7 against patches from offline bundles, which you import to the vSphere Lifecycle Manager depot manually.

You can stage patches before remediation to reduce host downtime.

Host Extension Remediation

During extension remediation, vSphere Lifecycle Manager does not automatically install the prerequisites of the extension. Missing extension prerequisites cause some remediation operations to fail. If the missing prerequisite is a patch, you can add it to a patch baseline. If the missing prerequisite is an extension, you can add it to the same or another extension

baseline. You can then remediate the host against the baseline or baselines that contain the prerequisite and the original extension baseline.

Remediating Hosts in a Cluster

For ESXi hosts in a cluster, the remediation process is sequential by default.

When you remediate a cluster of hosts sequentially and one of the hosts fails to enter maintenance mode, vSphere Lifecycle Manager reports an error and the remediation process stops and fails. The hosts in the cluster that are remediated stay at the updated level. The ones that are not remediated after one host fails remain unupdated.

The host upgrade remediation of ESXi hosts in a cluster proceeds only if all hosts in the cluster can be upgraded.

If you initiate remediation at a data center level, the remediation processes for the clusters run in parallel. Clusters that you manage with a single vSphere Lifecycle Manager image are not remediated against the attached baselines or baseline groups. If the remediation process fails for one of the clusters within a data center, the remaining clusters are still remediated.

Before you start remediation, you can generate a report that shows which cluster, host, or virtual machine has the cluster features enabled. For more information, see Remediation Pre-Check Report.

Remediation and Cluster Settings

If a host in a DRS-enabled cluster runs a virtual machine on which vCenter Server is installed, DRS first attempts to migrate the virtual machine running vCenter Server to another host, so that the remediation succeeds. If the virtual machine cannot be migrated to another host, the remediation fails for the host, but the remediation process for the cluster does not stop. vSphere Lifecycle Manager proceeds to remediate the next host in the cluster.

Remediation of hosts in a cluster requires that you temporarily deactivate cluster features such as VMware DPM and HA admission control. Also, you must turn off Fault Tolerance if it is enabled on any of the virtual machines on a host, and disconnect the removable devices connected to the virtual machines on a host, so that they can be migrated with vMotion. For more information about configuring the vSphere Lifecycle Manager remediation settings, see Configuring the vSphere Lifecycle Manager Remediation Settings.

If a vCenter HA failover is initiated during the remediation of a cluster, the remediation task is canceled. After the failover finishes, you must restart the remediation task on the new node.

When you perform remediation on a cluster that consists of not more than two hosts, disabling HA admission control might not be enough to ensure successful remediation. You might need to deactivate vSphere High Availability (HA) for the cluster. If you keep HA enabled, the remediation attempts on hosts in the cluster fail, because HA cannot provide recommendation to vSphere Lifecycle Manager to place any of the hosts into maintenance mode. The reason is that if one of the two hosts is placed into maintenance mode there is no failover host left available in the cluster. To ensure successful remediation on a two-node cluster, you must deactivate HA for the cluster or place the hosts in maintenance mode manually and then remediate the two hosts in the cluster.

vSAN Clusters

vSphere Lifecycle Manager remediates hosts that are part of a vSAN cluster sequentially. The reason is that by design only one host from a vSAN cluster can be in a maintenance mode at any time. For more information about using vSphere Lifecycle Manager with vSAN clusters, see vSAN Clusters and vSphere Lifecycle Manager.

Remediating Hosts That Contain Third-Party Software

Hosts might contain third-party software, such as Cisco Nexus 1000V VEMs or EMC PowerPath modules. When you upgrade an ESXi 6.5 or ESXi6.7 host to ESXi7.0, all supported custom VIBs are migrated and remain intact, regardless of whether the VIBs are included in the installer ISO.

If the host or the installer ISO image contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the VIB that creates the conflict.

To discover potential problems with third-party software before an upgrade operation, scan the hosts against an upgrade baseline and review the scan messages in the vSphere Lifecycle Manager compliance view. See Host Upgrade Compliance Messages and Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present.

For information about upgrading with third-party customization, see the *VMware ESXi Upgrade* documentation.

For information about using vSphere ESXi Image Builder to make a custom ISO, see the *VMware ESXi Installation and Setup* documentation.

Remediating ESXi 6.5 or ESXi6.7 Hosts Against an ESXi7.0 Image

When you upgrade an ESXi 6.5 or ESXi6.7 host to ESXi7.0, all supported custom VIBs remain intact on the host after the upgrade, regardless of whether the VIBs are included in the installer ISO.

When you perform a compliance check, the target host is scanned against a set of VIBs from the upgrade image. If you check the compliance of a host against an upgrade baseline that contains an ISO image of the same version as the target host, vSphere Lifecycle Manager displays Compliant or Non-compliant compliance status. If the upgrade image is the basic one distributed by VMware, or is a custom ISO image that contains the same set of VIBs as the ones already installed on the target host, the scan result is Compliant. If the upgrade ISO contains VIBs that are of different kind or version than the VIBs that are already on the target host, the scan result is Non-compliant.

The remediation process of an ESXi 6.5 or ESXi6.7 host against an ESXi7.0 image is an upgrade process.

Note: Upgrading to ESXi7.0 requires a boot device that is a minimum of 4 GB. When booting from a local disk, SAN or iSCSI LUN, up to 128 GB of disk space is used to create ESXi system partitions. You can create a VMFS datastore on a boot disk larger than 128 GB.

You can use an ISO 7.0 image in an upgrade operation of an ESXi7.0 host. The remediation process of ESXi7.0 host by using ESXi7.0 image with additional VIBs is equivalent to a patching process. Because the upgrade image is of the same version as the target host, upon completing the upgrade operation, the additional VIBs are added to the target host.

Table 124: Scan and Remediation Situations for ESXi 6.5 and ESXi6.7 Hosts Against ESXi7.0 Images

Action	Description
Compliance check and remediation of ESXi 6.5 or ESXi6.7 hosts against an ESXi7.0 image that contains additional non-conflicting and non-obsoleting VIBs with the target host.	vSphere Lifecycle Manager displays a Non-Compliant compliance status for the host. Remediation succeeds. All VIBs on the target host before remediation remain on the host. All VIBs from the upgrade image that are not present on the target host before remediation are added to the host.
Compliance check and remediation of ESXi 6.5 or ESXi6.7 hosts against an ESXi7.0 image that contains VIBs of a version later than the version of the same VIBs on the target host.	vSphere Lifecycle Manager displays a Non-Compliant compliance status for the host. Remediation succeeds. VIBs on the target host are updated to the later version.
Compliance check and remediation of ESXi 6.5 or ESXi6.7 hosts against an ESXi7.0 image that contains conflicting VIBs with the target host.	vSphere Lifecycle Manager displays an Incompatible compliance status for the host. Remediation fails. The host remains intact.
Scan and remediation of ESXi 6.5 or ESXi6.7 hosts against an ESXi7.0 image that contains vendor-tagged VIBs.	• If the vendor-tagged VIBs do not match the host hardware, vSphere Lifecycle Manager displays an Incompatible compliance status for the host. Remediation fails. • If the vendor-tagged VIBs match the host hardware, vSphere Lifecycle Manager displays a Non-Compliant compliance status for the host and remediation succeeds.

Action	Description
Scan and remediation of ESXi 6.5 or ESXi6.7 hosts against an ESXi7.0 image that contains VIBs that obsolete the VIBs installed on the host.	Remediation succeeds. All VIBs that have been installed on the target host before remediation are replaced by the newer VIBs from the ESXi image.

Remediation Pre-Check Report

The remediation pre-check report shows the results of a check that is performed on a cluster or a host before remediation. During that check, vSphere Lifecycle Manager identifies possible issues that might prevent successful remediation. Depending on the type of issue, vSphere Lifecycle Manager suggests actions that you must take to fix the issue or resolves the issue automatically.

You can generate a pre-check remediation report in the vSphere Lifecycle Manager compliance view for an object.

Table 125: Cluster Issues

Current Configuration/Issue	Recommended Action	Details
DRS is deactivated on the cluster.	Enable DRS on the cluster.	DRS enables vCenter Server to place and migrate virtual machines automatically on hosts to attain the best use of cluster resources.
vSAN health check fails during the pre-check.	Navigate to the vSAN Health page and address any health issues before proceeding with remediation.	The vSAN health check performs a series of tests on the hosts in the vSAN cluster. The vSAN health check must succeed to ensure the hosts are successfully remediated. If you start a remediation task in a vSAN cluster that failed the vSAN health check during the remediation pre-check, the hosts enter maintenance mode, get upgraded, but might fail to exit maintenance mode. The remediation eventually fails.
Insufficient licenses for one or multiple ESXi hosts in the cluster.	Ensure that you have multiple licenses for the ESXi hosts that have more than 32 cores per CPU.	One CPU license covers up to 32 physical cores. If a CPU has more than 32 cores, you must assign additional CPU licenses to the respective ESXi host. For more information, see https://www.vmware.com/company/news/updates/cpu-pricing-model-update-feb-2020.html.
DPM is enabled on the cluster.	None. vSphere Lifecycle Manager deactivates DPM automatically.	If a host has no running virtual machines, DPM might put the host in standby mode before or during remediation and vSphere Lifecycle Manager cannot remediate them.
HA admission control is enabled on the cluster.	None. vSphere Lifecycle Manager deactivates HA admission control automatically.	HA admission control prevents the migration of virtual machines with vSphere vMotion and the hosts cannot enter maintenance mode.

Current Configuration/Issue	Recommended Action	Details
EVC is deactivated on the cluster.	None. vSphere Lifecycle Manager enables EVC automatically, although no notification or message appears in the vSphere Client.	If EVC is deactivated for a cluster, the migration of virtual machines with vSphere vMotion cannot proceed. The result is downtime of the machines on the hosts that you remediate with vSphere Lifecycle Manager.

Table 126: Host Issues

Current Configuration/Issue	Recommended Action	Details
A CD/DVD drive is attached to a virtual machine on the ESXi host.	Disconnect the CD/DVD drive.	Any CD/DVD drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
A floppy drive is attached to a virtual machine on the ESXi host.	Disconnect the floppy drive.	Any floppy drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
Fault Tolerance (FT) is enabled for a virtual machine on the ESXi host.	Deactivate FT for the virtual machine.	If FT is enabled for any of the virtual machines on a host, vSphere Lifecycle Manager cannot remediate that host.
A powered on virtual machine is configured to use Virtual Flash Read Cache.	Deactivate Virtual Flash Read Cache before proceeding with the upgrade.	Virtual Flash Read Cache is not supported. During an upgrade operation, vSphere Lifecycle Manager removes Virtual Flash Read Cache for all virtual machines on the host. Before remediation, consult https://kb.vmware.com/s/article/2057840.
VMware vCenter Server is installed on a virtual machine on the ESXi host and DRS is deactivated on the cluster.	Enable DRS on the cluster and ensure that virtual machines can be migrated with vSphere vMotion.	One of the virtual machines in the cluster runs the vCenter Server instance that you currently use. If you enable DRS on the cluster, vSphere vMotion can migrate the virtual machine where vCenter Server runs to ensure that the remediation of the hosts is successful.
An ESXi host in the cluster has a CPU with more than 32 cores and requires multiple licenses.	Assign as many licenses as the host needs.	One CPU license covers up to 32 physical cores. If a CPU has more than 32 cores, you must obtain additional CPU licenses. For more information, see https://www.vmware.com/company/news/updates/cpu-pricing-model-update-feb-2020.html.

Generate a Pre-Remediation Check Report

When you generate a pre-remediation check report, vSphere Lifecycle Manager generates a list with actions that you must perform to ensure successful remediation of the hosts in your cluster.

The remediation pre-check report contains information about issues at the cluster, host, and VM level that might prevent the completion of remediation.

For information about the possible issues that might prevent successful remediation, see Remediation Pre-Check Report.

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Host** > **Baselines**.
3. In the **Baselines** pane, click **Pre-Check Remediation**.
   The **Remediation Pre-check** dialog box opens.
4. Review the results from the pre-check and click **Done**.
   In the bottom pane of the **Remediation Pre-check** dialog box, you see a list of issues at the host and virtual machine level.

The **Remediation Pre-check** dialog box lists the issues with cluster, hosts, and virtual machines that might prevent successful remediation of the selected object.

In the upper pane of the **Remediation Pre-check** dialog box, you see a list of issues at a cluster level.

In the bottom pane of the **Remediation Pre-check** dialog box, you see a list of issues at the host and virtual machine level.

Fix all issues that vSphere Lifecycle Manager identifies during the pre-remediation check and remediate the selected object.

Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines

Remediation makes the remediated ESXi host compliant with the attached baselines and baseline groups. You can remediate a host against a single or multiple baselines, or against a baseline group. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines. You can remediate ESXi hosts against a single attached upgrade baseline at a time.

- Required privileges: **VMware vSphere Lifecycle Manager** > **Manage Patches and Upgrades** > **Remediate to Apply Patches, Extensions, and Upgrades**.
- Attach a patch, upgrade, or extension baseline or a baseline group containing patches, upgrades, and extensions to the host.
- Resolve any issues that occur during Remediation Pre-check.
- In upgrade scenarios, verify that the ESXi hosts to upgrade have a boot disk of at least 4 GB. When booting from a local disk, SAN or iSCSI LUN, up to 128 GB of disk space is used to create ESXi system partitions. You can create a VMFS datastore on a boot disk larger than 128 GB.

You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline that contains an ESXi image. You can remediate a single ESXi host or a group of ESXi hosts in a container object, such as a folder, a cluster, or a data center. You can also initiate remediation at a vCenter Server level.

Note: Because the official VMware online depot hosts certified partner content in addition to VMware content, a broader set of OEM bulletins are available in the vSphere Lifecycle Manager depot. As a result, a broader set of OEM bulletins are included in the vSphere Lifecycle Manager predefined bulletins. During remediation, always inspect the contents of those

baselines to exclude the bulletins that you do not need in the baseline. For the bulletins that you do need, consult the corresponding KB articles for information about deployment specifics and dependencies. Verify that dependent bulletins are also included in the baselines that you use for remediation.

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a) Navigate to a host, cluster, or a container object.
   b) Click the **Updates** tab.
2. Select **Hosts** > **Baselines**.
3. In the **Attached Baselines and Baseline Groups** pane, select the baselines and baseline groups to use for remediation.

   You can select a single baseline or baseline group. You can also select multiple baselines and baseline groups. Your selection must contain no more than one upgrade baseline.
4. Click **Remediate**.

   If the selected baselines and baseline groups do not contain an upgrade image, the **Remediate** dialog box opens.

   If the selected baselines and baseline groups contain an upgrade image, the **End User License Agreement** dialog box opens.
5. To proceed to remediation, accept the terms and the license agreement in the **End User License Agreement** dialog box.

   After you accept the agreement and click **OK** to close the dialog box, the **Remediate** dialog box opens.
6. Expand the list of pre-check issues and review the actions that vSphere Lifecycle Manager must perform to ensure successful remediation.
7. Optional: To generate a full remediation pre-check report, click **Show Full Remediation Pre-Check Report**.

   If you select this option, the **Remediate** dialog box closes and vSphere Lifecycle Manager does not proceed with the remediation process. Instead, the **Remediation Pre-Check** dialog box opens. After you review the results from the remediation pre-check, you must initiate remediation again.
8. Expand the list of hosts to be remediated and deselect any host that you do not want to remediate.

   The list contains all the hosts to which the selected baselines and baseline groups are attached. Even if you navigated to a single host before initiating remediation, the list might still display multiple hosts to be remediated. All hosts in the list are selected by default. Deselecting hosts from the list changes the overall number of hosts to be remediated.
9. Optional: To view information about the updates that will be installed during the remediation, expand the list of updates.

   If the selection of baselines and baseline groups contains an upgrade baseline, information about the ESXi image is also displayed.
10. Optional: To schedule the remediation task for a later time, expand **Scheduling Options** and configure a scheduled remediation task.

    By default, the remediation task starts immediately after closing the **Remediate** dialog box.

11. Expand **Remediation settings** and review and edit the remediation settings.
    - To turn on or turn off Quick Boot, select or deselect the respective check box in the **Remediation settings** table.
    - To allow or disallow health checks after remediation, select or deselect the respective check box in the **Remediation settings** table.
    - To ignore warnings about unsupported hardware devices, select the respective check box in the **Remediation settings** table.
    - To configure parallel remediation for the selected hosts, expand **Parallel remediation**, select the respective check box and configure the maximum number of concurrent remediations.

      Note: vSphere Lifecycle Manager remediates in parallel only the ESXi hosts that are in maintenance mode. Hosts that are not in maintenance mode are not remediated. If you do not set the maximum number of concurrent remediations, vSphere Lifecycle Manager remediates all hosts that are in maintenance mode.

      If the hosts have NSX virtual distributed switches that are ready to be migrated to vSphere Distributed Switches, you must set the maximum number of parallel remediations to no more than 4. In cases when host switch migration is needed, if more than 4 hosts are remediated in parallel, the remediation might fail, because the host switch migration takes more time than the time vSphere Lifecycle Manager needs to complete the parallel remediation.
    - To change any other of the remediation settings, click the **Close Dialog And Go To Settings** link above the table.

      If you select this option, the **Remediate** dialog box closes and vSphere Lifecycle Manager does not proceed with the remediation process. Instead, you are redirected to the **Baselines Remediation Settings** pane on the **Settings** tab of the vSphere Lifecycle Manager home view. To change any of the remediation settings, click the **Edit** button. Remediation does not resume automatically. After you make the desired changes, you must initiate remediation again.
12. Click **Remediate**.

Depending on the remediation schedule you configure, the remediation task starts immediately or runs later.

Using vSphere Lifecycle Manager to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch

Starting with vSphere 7.0, the vSphere Distributed Switch supports the NSX functionality. For clusters enabled with VMware NSX-T Data Center™, you can migrate the NSX-managed Virtual Distributed Switches on the hosts to vSphere Distributed Switches during an upgrade of a cluster against a vSphere Lifecycle Manager baseline group that contains an ESXi image and NSX VIBs .

Migrating your host switch to vSphere Distributed Switch 7.0 ensures optimal pNIC usage, and lets you manage the networking for your NSX hosts from vCenter Server.

During an upgrade remediation, vSphere Lifecycle Manager checks if an NSX virtual distributed switch is present on each of the hosts in the cluster and if it is ready to be migrated. To prepare the NSX virtual distributed switch for migration, you must run the Upgrade Readiness Tool before upgrading the cluster. If the NSX distributed switch on any of hosts in the cluster is not ready to be migrated to a vSphere Distributed Switch, you cannot proceed with the remediation process. In this case, you need to go to NSX Manager and run the Upgrade Readiness Tool.

Requirements

- ESXi 7.0 Update 2
- vCenter Server 7.0 Update 2
- VMware NSX-T Data Center™ 3.1.1

As a good practice, contact VMware support to assess the impact of migrating to vSphere Distributed Switch 7.0.

Workflow

1. In NSX Manager, use the Upgrade Readiness Tool to run the migration readiness pre-check, address any configuration issues, review the recommended topology, and apply the new topology.
   For more information about the steps you need to perform in NSX Manager, see "Migrate Host Switch to vSphere Distributed Switch" in the *NSX-T Data Center Administration* documentation.
2. Upgrade vCenter Server to version 7.0 Update 2.
   For more information about upgrading vCenter Server, see the *vSphere Upgrade* documentation.
3. Create a baseline group that contains an ESXi image version 7.0 Update 2 and the NSX kernel module for ESXi 7.0 .
   a. Import an ESXi 7.0 Update 2 ISO image to the vSphere Lifecycle Manager depot.
      For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.
   b. Create an upgrade baseline that contains the imported ISO image.
      For more information, see Create a Host Upgrade Baseline.
   c. From myvmware.com, download the NSX kernel module for ESXi 7.0.
   d. Import the downloaded NSX bundle to the vSphere Lifecycle Manager depot.
      For more information, see Import Updates to the vSphere Lifecycle Manager Depot.
   e. Create an extension baseline that contains the imported kernel module.
      For more information, see Create a Host Extension Baseline
   f. Create a baseline group that contains the ESXi upgrade baseline and the extension baseline with NSX VIBs.
      For more information, see Create a Host Baseline Group.
4. Attach the baseline group to a cluster.
   For more information, see Attach Baselines and Baseline Groups to Objects.
5. Remediate the cluster against the attached baseline group.
   During the remediation, vSphere Lifecycle Manager upgrades the ESXi version first and then migrates the host switch, if migration is needed.
   For more information, see Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines.
6. If you use host profiles to configure the hosts in your environment, re-extract a new host profile from the reference host in the cluster.
   After the upgrade, due to the migration of the host switch, the existing host profiles become invalidated and inapplicable.
   For more information, see the *vSphere Host Profiles* documentation.

Using vSphere Lifecycle Manager Images

Using vSphere Lifecycle Manager images provides a simplified and unified workflow for patching and upgrade of ESXi hosts. You can also use vSphere Lifecycle Manager images for bootstrapping purposes and firmware updates.

An image defines the exact software stack to run on all ESXi hosts in a cluster.

General Workflow

Using images to apply software and firmware updates to ESXi hosts is a multi-stage process.

1. Software updates must become available in the vSphere Lifecycle Manager depot.
   To set up and use an image, you use the software updates that are available in the vSphere Lifecycle Manager depot. The depot contains base images, vendor add-ons, and additional components.
   Updates get into the vSphere Lifecycle Manager local depot through synchronization with configurable download sources. By default, vSphere Lifecycle Manager is configured to synchronize with the official VMware depot. You can also import updates into the depot manually.
   You can see the contents of the vSphere Lifecycle Manager depot in the vSphere Lifecycle Manager home view.
   For more information, see Working with the vSphere Lifecycle Manager Depot.

2. Start using vSphere Lifecycle Manager images.
   vSphere Lifecycle Manager provides you with the option to start using images with the very creation of a cluster. If you do not set up an image during the creation of a cluster, you can switch from using vSphere Lifecycle Manager baselines to using vSphere Lifecycle Manager images at a later time.
   Even when you save the image, no software is installed on the ESXi hosts during image setup.
   For more information, see Creating vSphere Lifecycle Manager Clusters and Switching from Using Baselines to Using Images.
3. Check the compliance of the ESXi hosts in the cluster against the image specification.
   The compliance check compares the current image on the ESXi hosts in the cluster against the desired image that you specified during the setup process, and defines compatibility status of the hosts.
   For more information, see Check Cluster Compliance Against an Image.
4. Review the compliance statuses of the hosts in the cluster.
5. You can run a remediation pre-check on an ESXi host to ensure software and hardware compatibility with the image.
   Running a remediation pre-check is optional. The remediation pre-check ensures that all requirements for successful remediation are met. For more information, see Run a Remediation Pre-Check for a Cluster.
6. Remediate the non-compliant ESXi hosts in the cluster.
   Remediation is the process through which the software specification defined by the vSphere Lifecycle Manager image that you use for a cluster is actually applied to the hosts in the cluster.
   For more information about remediating hosts against an image, see Remediate a Cluster Against a Single Image.

Limitations

- When you set up and save an image for a cluster, the image is not applied to the hosts in the cluster unless you remediate the hosts. The mere action of changing the management method does not alter the hosts in the cluster.
- After you set up an image for the cluster and remediate the hosts in the cluster against the image, standalone VIBs are deleted from the hosts.
- After you set up an image for the cluster and remediate the hosts in the cluster against the image, non-integrated solution agents are deleted from the hosts.

Working with Images

When you manage a cluster with a single image, you can change the image at any time. You can edit the image by changing the software that it includes, for example, you can add or remove components, and you can also change the version of the included components.

Using vSphere Lifecycle Manager images starts with setting up an image for a cluster. You can set up an image during the creation of the cluster or later.

After you start managing a cluster with a single image, you can edit the image at any time. You can validate the image before saving it to verify that it includes no conflicting components or missing dependencies.

You can export and import images. For example, you can export an image as an installable ISO file, which you can use for bootstrapping purposes. You can also export the image as a JSON file and reuse it for another cluster that uses images.

Setting Up an Image

To take advantage of all new functionalities that vSphere Lifecycle Manager provides in vSphere 7.0, for example, software recommendations and firmware updates, you must start using images for the clusters in your environment. You can set up an image during the creation of a cluster or later.

During the creation of a cluster, you can only define the ESXi version and, optionally, a vendor add-on to be included in the image for the cluster. You can later edit the image to include additional components or a firmware add-on. For detailed information about creating a cluster and adding hosts to it, see the *vCenter Server and Host Management* documentation.

Note: When you set up an image, you select an ESXi version and a vendor add-on from the vSphere Lifecycle Manager depot. If no ESXi base images and vendor add-ons are available in the vSphere Lifecycle Manager depot, you must populate the depot with software updates by synchronizing the depot or uploading updates to the depot manually. For detail information about the corresponding procedures, see Synchronize the vSphere Lifecycle Manager Depot and Import Updates to the vSphere Lifecycle Manager Depot.

If you do not set up an image during the creation of the cluster, it uses baselines, but you can switch to images at any time. When you set up an image during the transition workflow, you can define the full stack of software to run on the hosts in the cluster. For more information about switching from baselines to images, see Switching from Using Baselines to Using Images.

Whereas switching from baselines to images is possible, the reverse operation is not. If a cluster uses a single image, regardless of whether you set up the image during the cluster creation or transition, you cannot switch to using baselines for that cluster.

Viewing Image Details

You can view details about the image that a cluster uses as well as compliance information for that cluster in the vSphere Lifecycle Manager compliance view.

You access the vSphere Lifecycle Manager compliance view from the **Updates** tab for a cluster.

The **Image** pane consists of two cards.

The **Image** card contains information about the image that the cluster uses. In that card, you perform all image-related operations. You edit the image, you export the image, you validate your selections, and so on. You can also check and view the recommendations that VMware provides.

The **Image Compliance** card contains compliance information about the hosts in the cluster. In that card, you perform host-related operations. You check the compliance of the hosts in the cluster, you run remediation pre-checks, you remediate the hosts, and so on.

In the **Image Compliance** card, you edit remediation settings for that cluster and manage depot overrides.

Editing Images

For a cluster that you manage with a single image, you can edit the image at any time to add, remove, or update an image element. For example, you can edit the image to update the vendor add-on version that it includes, to add or remove a driver, to upgrade the ESXi version in the image, and so on.

Working with Drafts

When you edit an image, vSphere Lifecycle Manager saves the working copy of the image as a draft. The draft is an edited but unsaved version of an image. If you edit an image but for some reason you do not save the new image set-up, when you restart editing the image, you can use the saved draft version as a starting point or you can altogether discard the changes that you previously made.

Validation

You can validate an image draft before you save it. Validation checks whether the image is correct and complete. During validation, vSphere Lifecycle Manager checks for missing dependencies and conflicting components. In case of issues, vSphere Lifecycle Manager returns messages with information about the existing issues. You must resolve all issues before you can save the image.

Edit an Image

If a cluster uses a single image, you can edit that image at any time. You can add, remove, or modify the elements included in the image.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image** card, click the **Edit** button.
4. In the **Edit Image** card, modify the image set-up.

Image Element	Possible Modifications
ESXi Version	From the **ESXi Version** drop-down menu, select a new ESXi base image.
Vendor Add-On	• To add a vendor add-on to the image, click **Select** and select a vendor add-on. • To change the version of the vendor add-on in the image or to select a new vendor add-on, click the pencil icon and make your changes . • To remove the vendor add-on from the image altogether, click the trash icon .
Firmware and Drivers Add-On	• To add a firmware add-on to the image, click **Select**. In the **Select Firmware and Drivers Addon** dialog box, specify a hardware support manager and select a firmware add-on to add to the image. • To select a new firmware add-on, click the pencil icon and make your changes. • To remove the firmware add-on element from the image altogether, click the trash icon. Selecting a firmware add-on for a family of vendor servers is possible only if the respective vendor-provided hardware support manager is registered as an extension to the vCenter Server where vSphere Lifecycle Manager runs.
Components	Click **Show details** and view the list of additional components in the image. • To add components to the image, click **Add Components** and select the components and their corresponding versions to add to the image. • To delete a component from the image, click the trash icon in the table with components. • To delete a manually added component that overrides a component in the selected vendor add-on or base image, click the undo icon in the table with components. This action reverts the override.

5. Optional: To validate the image, click the **Validate** button.
   You validate an image to check for missing dependencies and component conflicts.

6. Click **Save**.

   The save operation triggers validation. If the image is valid, vSphere Lifecycle Manager saves it and runs a compliance check against the new image. You can view compliance information in the **Image Compliance** card.

   If the image is invalid, saving the image fails and vSphere Lifecycle Manager returns an error.

The new image is validated and displayed in the **Image** card. vSphere Lifecycle Manager performs an automatic hardware compatibility check against the new image.

If there are recommended images generated for the cluster, those recommendations become invalidated and updated. vSphere Lifecycle Manager automatically generates a new recommendation based on the new image.

Reusing Existing Images

A vSphere Lifecycle Manager image can be distributed within the same vCenter Server instance where vSphere Lifecycle Manager runs or across vCenter Server instances. You can reuse an image that you already set up by exporting it from its cluster and importing it to the target cluster.

To reuse an existing image for a cluster in the same vCenter Server system, you must export the image as a JSON file and then import the JSON file to the target cluster.

However, when you want to use an existing image for a cluster in another vCenter Server instance, exporting the image as a JSON file might not be enough. You might also need to export the image as a ZIP file. At the target location, you must import the JSON file as an image to the target cluster. You might also need to import the ZIP file to the target vSphere Lifecycle Manager depot to make sure that all components included in the image are available to the target vSphere Lifecycle Manager instance.

Distribution Formats for vSphere Lifecycle Manager Images

You can use vSphere Lifecycle Manager to customize an ESXi base image by adding vendor add-ons and additional components. Depending on your goal, a vSphere Lifecycle Manager image can be distributed and consumed in three different formats.

ISO Image

Distributing an image created with vSphere Lifecycle Manager in an ISO format is useful when you need the image to perform clean installs of ESXi and for bootstrapping purposes, for example the kickstart workflow.

You cannot use an image exported as an ISO file with another cluster that uses vSphere Lifecycle Manager images.

You can import the ISO image into the local depot of the target vSphere Lifecycle Manager instance, but you can only use the ISO file to create upgrade baselines. You cannot use ISO files with vSphere Lifecycle Manager images.

ZIP File

Distributing an image created with vSphere Lifecycle Manager as an offline bundle is useful when you want to import the components that the image contains into the depot of the target vSphere Lifecycle Manager instance.

Unlike the ISO image, you cannot use a ZIP file to create upgrade baselines.

JSON File

Distributing an image created with vSphere Lifecycle Manager as a JSON file is useful when you want to reuse the same image for other clusters that use images for host management.

When you distribute the JSON file to clusters in a different vCenter Server instance, you must make sure that the depot of the target vSphere Lifecycle Manager instance contains all components that the JSON file contains.

The JSON file contains only metadata and not the actual software payloads.

Export an Image

You export an image when you want to use the same image for another cluster in the same or in a different vCenter Server instance.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Depending on your goals, you can export an image in three different formats. You can export the image as a JSON file, as an installable ISO image, or as an offline bundle that contains all software packages included in the image. For more information about the different distribution formats, see Distribution Formats for vSphere Lifecycle Manager Images.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. Click the horizontal ellipsis icon and select **Export**.
4. In the **Export Image** dialog box, select a file format, and click **Export**.
   You can export the image in one file format at a time. The export format depends on your needs and goals.

   If you intend to use the image for a cluster in another vCenter Server, you must export it as a JSON file and as a ZIP file. Afterwards, you must import both the JSON file and the ZIP file to the target vCenter Server system.

The exported file is saved on your local machine.

Import the image to a target cluster in the same or in a different vCenter Server instance. For more information, see Import an Image .

For information about importing updates to the vSphere Lifecycle Manager depot, see Import Updates to the vSphere Lifecycle Manager Depot.

Import an Image

Instead of setting up a new image manually, you can reuse an existing image by importing it to a cluster. Upon remediation, the imported image is applied to all hosts in the cluster.

- Verify that the vSphere Lifecycle Manager depot contains all components included in the image that you import.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

You can import an image only if it is in a JSON format. The JSON file contains only the image metadata, but not the actual software payloads. To successfully import an image to a cluster and apply the software specification to the hosts in the cluster, all the components must specified in the image be available in the vSphere Lifecycle Manager depot.

So, if you want to distribute and reuse an image across vCenter Server instances, importing the JSON file might not be enough if the components from the image are not available in the target vSphere Lifecycle Manager depot. In such cases, before you import the JSON file to the target cluster, you must first import to the target vSphere Lifecycle Manager depot an offline bundle that contains all components included in the image. If you try to import a JSON file to a cluster but the target vSphere Lifecycle Manager depot does not contain the corresponding components, the import operation fails due to validation errors.

For information about importing updates to the vSphere Lifecycle Manager depot, see Import Updates to the vSphere Lifecycle Manager Depot.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. Click the horizontal ellipsis icon and select **Import**.
4. In the **Import Image** dialog box, select a JSON file and click **Next**.
   - Enter a URL address to the JSON file that you want to import.
   - Browse to a JSON on your local machine.
5. Optional: In the **Edit Image** card, modify the image set-up.

Image Element	Possible Modifications
ESXi Version	From the **ESXi Version** drop-down menu, select a new ESXi base image.
Vendor Add-On	• To add a vendor add-on to the image, click **Select**. • To change the version of the vendor add-on in the image or to select a new vendor add-on, click the pencil icon. • To remove the vendor add-on element from the image altogether, click the trash icon .
Firmware and Drivers Add-On	• To add a firmware add-on to the image, click **Select**. • To select a new firmware add-on, click the pencil icon. • To remove the firmware add-on element from the image altogether, click the trash icon. Selecting a firmware add-on for a family of vendor servers is possible only if the respective vendor-provided hardware support manager is registered as an extension to the vCenter Server where vSphere Lifecycle Manager runs.
Components	Click **Show details** and view the list of additional components in the image. • To add components to the image, click **Add Components** and select components to add to the image. • To delete a component from the image, click the trash icon in the table with components. • To delete a manually added component that overrides a component in the selected vendor add-on, click the undo icon in the table with components. This action reverts the override.

6. If the image contains conflicting components or unresolved dependencies, resolve the issues and retry the procedure.
7. Optional: To validate the image, click the **Validate** button.
   You validate an image to check for missing dependencies and component conflicts.
8. Click **Save**.
   A compliance check task is automatically triggered. You can view compliance information in the **Image Compliance** card.

The imported JSON file is imported and set as your new image for the target cluster. At that stage, nothing is installed on the hosts in the cluster. The installation of software on the hosts happens during remediation.

Remediate the hosts in the cluster against the new image. See Run a Remediation Pre-Check for a Cluster and Remediate a Cluster Against a Single Image.

Checking Compliance Against a Single Image

When you check the compliance of a cluster against an image, vSphere Lifecycle Manager compares the software on each host in the cluster with the software specified in the image. If the image contains a firmware and drivers add-on, the compliance check also calculates the firmware compliance of the hosts with the image.

For example, vSphere Lifecycle Manager compares the ESXi version on each host to the ESXi version in the image for the cluster.

In addition to calculating the compliance state for each host, the compliance check gives you information about the impact that the remediate operation will have on a host, for example if remediation will cause host reboot or if maintenance mode is needed for the host.

Compliance information about the hosts in a cluster is displayed on the **Updates** tab for that cluster, in the **Image Compliance** card. The **Image Compliance** card displays a list of all hosts that are out of compliance with the image for the cluster. When you select a host, the compliance information about the host appears on the right.

Compliance States

During a compliance check, the software on each of the hosts in a cluster is compared to the software specification in the image that you set up for the entire cluster. The compliance check defines the compliance of each host with the image for the cluster.

A host can have any of the four compliance states: compliant, non-compliant, incompatible, and unknown.

Compliant

A host is complaint if the image on the host matches the image that you set for the cluster.

Non-Compliant

A host is non-compliant if the image on the host does not match the image that you set for the cluster. A compliant host becomes non-compliant when you set a new image for the cluster or manually add or remove components on the host. You remediate non-compliant hosts to make them compliant.

For example, a host is non-compliant in the following cases.

- The ESXi version on the host is earlier than the ESXi version included in the image for the cluster.
- The firmware on the host is different from the firmware add-on in the image for the cluster.
- The host has a component that is not included in the image for the cluster.
- The host contains a standalone VIB.

Incompatible

A host is incompatible when the image for the cluster cannot be applied to the host.

For example, a host is incompatible in the following cases.

- The ESXi version on the host is later than the ESXi version included in the image for the cluster.
- The host does not have sufficient resources, for example RAM.
- The hardware of the host is incompatible with the vSphere Lifecycle Manager image for the cluster.

Unknown

The unknown compliance state indicates that there is no compliance information about the host.

For example, the compliance state of a host is unknown in the following cases.

- You add a new host to the cluster. The compliance state of the newly added hosts is unknown until you perform a compliance check operation on the cluster.

- You edit the image for the cluster and save the modifications. The compliance state of all hosts in the cluster is unknown until you check the compliance of the cluster against the new image.

Check Cluster Compliance Against an Image

You check the cluster compliance against an image to understand how each of the hosts in the cluster compares to the specified image.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

When you perform the check compliance operation on an object that contains multiple clusters that you manage with a single image, for example a data center or vCenter Server instance, vSphere Lifecycle Manager performs compliance checks on all those clusters.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the **Check Compliance** button.

The **Image Compliance** card displays information about the overall number of non-compliant and incompatible hosts in the cluster. The **Image Compliance** card also displays a list of all hosts that are not compliant with the image for the cluster, so that you can view detailed compliance information about those hosts. The information panel appears on the right.

Remediate the cluster to make the non-compliant hosts compliant. See Run a Remediation Pre-Check for a Cluster and Remediate a Cluster Against a Single Image.

View Host Compliance Information

You can view detailed compliance information for every non-compliant host in a cluster that you manage with a single image. As a result, you can easily find what causes the host to become out of compliance with the cluster image.

- Run a compliance check.
- Verify that no host is added to the cluster after your last compliance check.

Detailed compliance information is displayed only for hosts that are out of compliance with the image in the cluster. vSphere Lifecycle Manager displays no compliance details for compliant hosts.

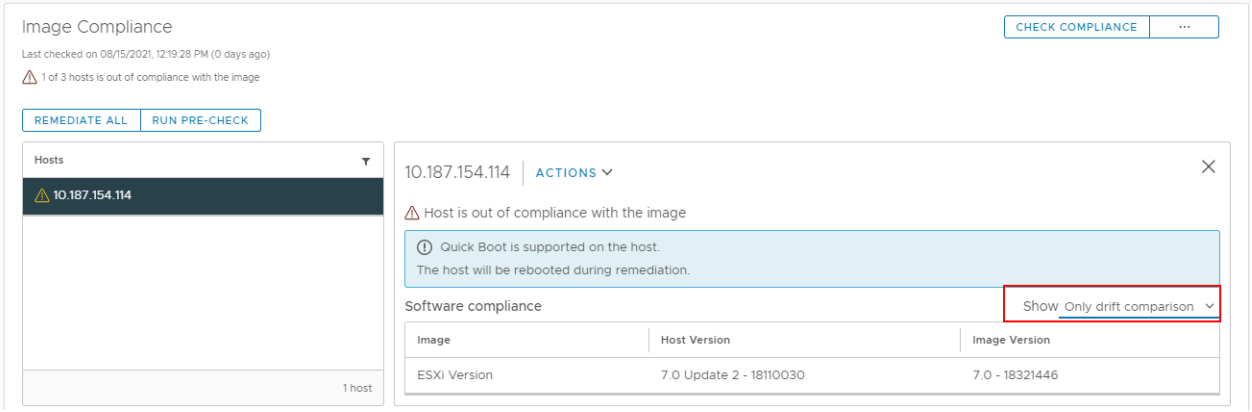
For hosts that have the incompatible compliance state, vSphere Lifecycle Manager shows in a signpost information about what causes the compatibility issues.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, select a host from the **Hosts** list.

   Note: Only non-compliant hosts are listed.

   An information panel appears on the right. In the **Software compliance** table, you can see what software runs on the selected host and what is the software specification in the image for the cluster.

4. To view the full comparison between the image on the host and the image for the cluster, select **Full image comparison** from the drop-down menu for the **Software compliance** table.
5. To view only the image elements that make the host non-compliant with the image for the cluster, select **Only drift comparison** from the drop-down menu for the **Software compliance** table.



Run a Remediation Pre-Check for a Cluster

To ensure that cluster health is optimal and that no problems occur during the remediation of the cluster against a single image, you can perform a remediation pre-check.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

The remediation pre-check operation includes a series of checks for the cluster and for each host in the cluster. These checks include extensive health checks to determine whether the cluster is in a stable state and to ensure successful remediation. Also, the remediation pre-check triggers a compliance check for the cluster. As a result, after the remediation pre-check, you can view compliance information for each host and whether host reboot or maintenance mode are necessary for successful remediation.

For vSAN clusters, the remediation pre-check operation includes a hardware compatibility check. Depending on how you configure the vSphere Lifecycle Manager remediation settings, vSphere Lifecycle Manager might prevent remediation if hardware compatibility issues exist.

For information about configuring the global vSphere Lifecycle Manager remediation settings, see Configure Remediation Settings for vSphere Lifecycle Manager Images . For information about configuring the remediation settings for a particular cluster, seeEdit the Remediation Settings for a Cluster.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the **Run pre-check** button.

   You can observe the progress of the pre-check task. When the task finishes, vSphere Lifecycle Manager displays information about the issues found during the pre-check.

If vSphere Lifecycle Manager reports no issues, remediate the cluster. See Remediate a Cluster Against a Single Image.

If issues are reported, resolve the issues before you remediate the cluster.

Run a Remediation Pre-Check for a Single Host

Instead of generating a remediation pre-check report for the entire cluster, you can run a remediation pre-check task for a single host in the cluster.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

The remediation pre-check task ensures that the host can be successfully remediated.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the vertical ellipsis icon for a host and select **Run pre-check**.
   The **Running pre-check** card appears. You can observe the progress of the task.

When the pre-check finishes, vSphere Lifecycle Manager displays information about the issues found during the pre-check.

If vSphere Lifecycle Manager reports no issues, you can remediate the host. See Remediate a Single Host Against an Image.

If vSphere Lifecycle Manager reports any issues, resolve the issues before you remediate the host.

Remediating a Cluster Against a Single Image

When you set up or import a vSphere Lifecycle Manager image to use with a cluster, the software specified in the image is not immediately installed on the hosts in that cluster. To apply the software specification from the image to the hosts, you must remediate the cluster against that image.

To initiate remediation of a cluster, you must have the required privileges. For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Images. For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation

During the remediation of a cluster against a vSphere Lifecycle Manager image, the ESXi hosts in the cluster are remediated sequentially. So, if the remediation for a single host in the cluster fails, the remediation of the entire cluster stops. Parallel remediation is an option only supported if you manage a cluster with vSphere Lifecycle Manager baselines.

During remediation, the image that you set up for the cluster is installed on all ESXi hosts in the cluster.

When you remediate a cluster that contains a single ESXi host or that has vSphere DRS deactivated or in manual mode, the remediation process cannot put that host into maintenance mode. So, to proceed with the remediation, you must power off the virtual machines that are running on the host, move them to another host, or select a user policy that allows the remediation process to power off the virtual machines. You can also set a user policy to power on the virtual machines after the host is remediated.

For vSAN clusters, the remediation operation includes a hardware compatibility check. Depending on how you configure the vSphere Lifecycle Manager remediation settings, vSphere Lifecycle Manager might not proceed with the remediation task if hardware compatibility issues exist. For information about configuring the global vSphere Lifecycle Manager remediation settings, see Configure Remediation Settings for vSphere Lifecycle Manager Images . For information about configuring the remediation settings for a particular cluster, see Edit the Remediation Settings for a Cluster.

Maintenance Mode

If the update requires it, hosts are put into maintenance mode before remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience, vCenter Server migrates the virtual machines to other hosts within the cluster before a host is put into maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for vMotion and if DRS and VMware Enhanced vMotion Compatibility (EVC) are enabled. EVC guarantees that the CPUs of the hosts are compatible, but it is not a prerequisite for vMotion.

You can configure vSphere Lifecycle Manager to deactivate HA admission control for the cluster before remediation. However, disabling HA admission control before you remediate a two-node cluster that uses a single vSphere Lifecycle Manager image causes the cluster to practically lose all its high availability guarantees. The reason is that when one of

the two hosts enters maintenance mode, vCenter Server cannot failover virtual machines to that host and HA failovers are never successful. For more information about HA admission control, see the *vSphere Availability* documentation.

Edit the Remediation Settings for a Cluster

You can customize the remediation settings for a particular cluster while the global remediation settings remain intact and applicable to all other clusters that you manage with vSphere Lifecycle Manager images.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

The vSphere Lifecycle Manager remediation settings define how ESXi hosts and virtual machines behave before and during a remediation of a cluster. You configure the vSphere Lifecycle Manager remediation settings in the vSphere Lifecycle Manager home view. The remediation settings are valid for all clusters in the vCenter Server instance where vSphere Lifecycle Manager runs. For more information about how to configure the vSphere Lifecycle Manager remediation settings, see Configure Remediation Settings for vSphere Lifecycle Manager Images .

Additionally, you can modify and override the global remediation settings for a single cluster. The overrides are used during the remediation of that specific cluster. For all other clusters, the global remediation settings apply.

For information about automatically triggered hardware compatibility checks, which is a functionality that is applicable only to vSAN clusters, see Automatically Triggered Hardware Compatibility Checks for vSAN Clusters.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the horizontal ellipsis icon and select **Edit remediation settings**.
4. In the **Edit Remediation Settings** dialog box, configure the remediation settings of the target cluster and click **Save**.

Option	Description
Quick Boot	Quick Boot reduces the host reboot time during remediation. Before you enable Quick Boot, you must make sure that the ESXi host is compatible with the feature.
VM power state	The **VM power state**option lets you control the behavior of the virtual machines that run on the ESXi host. You can select from the following options. • **Do not change power state** • **Suspend to disk** • **Suspend to memory** To select the **Suspend to memory** option, you must enable Quick Boot. Otherwise, the **Suspend to memory** option is dimmed. Together with Quick Boot, the **Suspend to memory** option provides faster host upgrades. vSphere Lifecycle Manager Together with Quick Boot, the **Suspend to memory** option provides faster host upgrades. vSphere Lifecycle Manager suspends to the host memory and not to the disk the powered on virtual machines on the host. After the Quick Boot, the suspended virtual machines are resumed from memory. • **Power off**
VM migration	You can configure vSphere Lifecycle Manager to migrate the suspended and powered off virtual machines from the hosts that must enter maintenance mode to other hosts in the cluster.
Maintenance mode failures	You can configure how vSphere Lifecycle Manager behaves if a host fails to enter maintenance mode before remediation. You

Option	Description
	can configure vSphere Lifecycle Manager to wait for a specified retry delay period and to retry to put the host into maintenance mode as many times as you indicate in the **Number of retries** text box.
HA admission control	Admission control is a policy that vSphere HA uses to ensure failover capacity within a cluster. If vSphere HA admission control is enabled during remediation, vMotion might be unable to migrate the virtual machines within the cluster. Disabling admission control allows a virtual machine to be powered on even if it causes insufficient failover capacity. When this happens, no warnings are presented, and the cluster does not turn red. If a cluster has insufficient failover capacity, vSphere HA can still perform failovers, and uses the VM Restart Priority setting to determine which virtual machines to power on first. **Note:** Disabling HA admission control before you remediate a two-node cluster causes the cluster to practically lose all its high availability guarantees. • If you select the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables HA admission control after remediation is complete. • If you deselect the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which HA admission control is enabled.
DPM	VMware Distributed Power Management (DPM) monitors the resources consumed by the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. • If you select the **Disable DPM on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables DPM after remediation is complete. • If you deselect the **Disable DPM on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which DPM is enabled.
Hardware compatibility issues	vSphere Lifecycle Manager performs a hardware compatibility check as part of the remediation pre-check and the remediation tasks for vSAN clusters. You can configure vSphere Lifecycle Manager to prevent remediation when hardware compatibility issues exist for the cluster. • If you select the **Prevent remediation if hardware compatibility issues are found** option, vSphere Lifecycle Manager reports hardware compatibility issues as an error, which prevents remediation. • If you deselect the **Prevent remediation if hardware compatibility issues are found** option, vSphere Lifecycle

Option	Description
	Manager reports hardware compatibility issues as a warning, which does not prevent remediation. If the cluster is not vSAN-enabled, vSphere Lifecycle Manager does not perform a hardware compatibility check as part of the remediation pre-check or the remediation tasks.

These settings become the remediation settings for the selected cluster. vSphere Lifecycle Manager uses those settings for that cluster for all future remediation tasks. The global remediation settings remain unchanged and are applied to all other clusters.

In the **Image Compliance** card, vSphere Lifecycle Manager displays a message that the global remediation settings are overridden. Also, an option to reset the values appears in the card.

Remediate a Cluster Against a Single Image

By remediating a cluster against an image, you apply the software specified in the image to all the hosts in the cluster. So, by remediating a cluster, you make the non-compliant hosts compliant with the image that you set for the cluster.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

During remediation, the hosts in the cluster are remediated in sequence. The hosts that have the incompatible compliance state are not remediated.

If a vCenter HA failover is initiated during the remediation of a cluster, the remediation task is canceled. After the failover finishes, you must restart the remediation task on the new node.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the **Remediate All** button.
   The **Review Remediation Impact** dialog box appears. The dialog box contains detailed information about all changes that remediation will enforce on the hosts in the cluster.
4. In the **Review Remediation Impact** dialog box, review the impact summary, the applicable remediation settings, and the EULA.
5. To save and review the impact details later, click **Export Impact Details**
6. Accept the EULA by selecting respective check box.
   The check box is selected by default.
7. Click the **Start remediation** button.
   The Remediate Cluster task appears in the **Recent Tasks** pane. You can also observe the progress of the remediation task in the **Image Compliance** card. If remediation fails, vSphere Lifecycle Manager gives information about the reasons for the failure.

Remediate a Single Host Against an Image

When you remediate a single host against the image for the cluster, vSphere Lifecycle Manager applies the image to that host only. Remediation is the operation that makes a non-compliant host in the cluster compliant with the image that you use for that cluster.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the vertical ellipsis icon for a host and select **Remediate**.
   The **Review Remediation Impact** dialog box appears. The dialog box contains detailed information about all changes that remediation will enforce on the host.
4. Review the impact summary, the applicable remediation settings, and the EULA.
5. To save and review the impact details later, click **Export Impact Details**
6. Accept the EULA by selecting respective check box.
   The check box is selected by default.
7. Click the **Start remediation** button.
   The Remediate Cluster task appears in the **Recent Tasks** pane. You can also observe the progress of the remediation task in the **Image Compliance** card. If remediation fails, vSphere Lifecycle Manager gives information about the reasons for the failure.

View Last Remediation or Remediation Pre-Check Results for a Cluster that Uses a Single Image

You can view the remediation results from the last remediation or remediation pre-check that vSphere Lifecycle Manager performed.

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the horizontal ellipsis icon and select your task.
   - To view the results from the last remediation pre-check performed on the cluster, select **Last pre-check results**.
   - To view the results from the last remediation of the cluster, select **Last remediation results**.

The **Image Compliance** displays detailed information about the last remediation or remediation pre-check task that ran on the cluster.

Manage Depot Overrides for a Cluster

Instead of accessing the vSphere Lifecycle Manager depot in vCenter Server, clusters in Remote Office and Branch Office (ROBO) deployments can download data from a depot that is local for them. You can configure vSphere Lifecycle Manager to use local depots for any cluster that uses images.

- Set up an online depot to which the cluster can connect.
- Export an offline bundle with components from a vSphere Lifecycle Manager image and import the offline bundle to the target local depot.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

A ROBO cluster is a cluster that has limited or no access to the Internet or limited connectivity to vCenter Server. As a result, clusters in ROBO deployments might have limited access to the vSphere Lifecycle Manager depot during the compliance check, remediation pre-check, and remediation operations.

With vSphere Lifecycle Manager images, you can use a local depot for ROBO clusters and configure vSphere Lifecycle Manager to use the local depot during the compliance check, remediation pre-check, and the remediation tasks. The local

depot overrides the vSphere Lifecycle Manager depot. Using local depots with ROBO clusters saves time and network bandwidth.

For each cluster that you manage with a single image, you can add and use multiple local depots instead of the default vSphere Lifecycle Manager depot. You can also delete the depot overrides that you configure. If depot overrides are not active for a cluster, the cluster uses the general vSphere Lifecycle Manager depot in vCenter Server.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image Compliance** card, click the horizontal ellipsis icon and select **Manage depot overrides**.
   The **Manage depot overrides** dialog box appears.
4. Select your task.

Option	Description
Add depot overrides	Enter a URL or a file path to a local depot and click **Add**. The depot is added to the **Depot override URL** list.
Delete a depot override	Click the horizontal ellipsis icon for a depot override from the list and click **Delete**. The depot is removed from the **Depot override URL** list.

5. Click **Close** .

In the **Image Compliance** pane, you see a notification if depot overrides are active for the cluster.

Recommended Images

For the clusters that you manage with images, vSphere Lifecycle Manager can generate and provide you with software recommendations in the form of pre-validated images that are compatible with the hardware of the hosts in a cluster. Recommended images are valid images that are based on the latest ESXi major or minor release.

When you set up or edit an image, you manually combine the image elements (ESXi version, vendor add-on, firmware add-on, and additional components) in such a way as to define the full software stack to run on all hosts in the cluster. You must manually check whether a particular image set-up is complete and valid, and suitable to your environment. The vSphere Lifecycle Manager recommendations save you the effort of exploring the possible and applicable combinations of image elements.

Recommended images are validated through a series of checks that ensure that a recommended image has no missing dependencies or conflicting components. For vSAN clusters, the validation also runs a hardware compatibility check against the vSAN Hardware Compatibility List (vSAN HCL). The extensive validation checks ensure that if you decide to use a recommended image for a cluster, the remediation against the recommended image is successful.

To generate recommendations, vSphere Lifecycle Manager checks what software is available in the vSphere Lifecycle Manager depot and what firmware is available in the depot that the selected hardware support manager makes available. Based on the available software, firmware, and, for vSAN clusters, the hardware compatibility checks, for each cluster that you manage with a single image, vSphere Lifecycle Manager provides you with up to two recommended images.

- Latest image
  The latest image contains the latest major ESXi version. For example, if the current image for a cluster contains a base image of version ESXi 7.0 and base images of version 7.5 and 8.0 are available in the vSphere Lifecycle Manager depot, the latest image recommendation contains ESXi version 8.0.
- Latest image in the current series
  The latest image in a series contains the latest minor ESXi. For example, if the current image for a cluster contains a base image of version ESXi 7.0 and base images of version 7.0a, 7.0 U1, 7.5, and 8.0 are available in the vSphere Lifecycle Manager depot, the latest image in the current series recommendation contains ESXi version 7.0 U1.

The ESXi version in a recommended image might be the same as the ESXi version in the current image for a cluster. But the recommended image might contain a later version of the vendor add-on, component, or firmware add-on.

Sometimes, the latest ESXi version available in the depot might not be recommended, because it causes hardware compatibility issues. In that cases, vSphere Lifecycle Manager reports that no recommended images are available for the cluster.

You can replace the current image of a cluster with one of the recommended images for that cluster.

The recommendation generation task is cancelable.

Automatically Triggered Recommendation Generation

vSphere Lifecycle Manager generates a new image recommendation automatically in the following cases.

- The vSphere Lifecycle Manager depot gets updated.
  By default, the depot updates every 24 hours. Also, the content of the depot changes when you import an offline bundle to the depot or you manually trigger synchronization to the configurable download sources.
- You edit the image that you use for a cluster and save the new image set-up.

Note: If the depot gets updated with solution components only, vSphere Lifecycle Manager does not generate new recommendations. Similarly, if you edit an image by only adding solution components to the image, vSphere Lifecycle Manager generates no new recommendation.

The automated recommendation generation is available only for clusters that already have recommended images generated. When vSphere Lifecycle Manager starts the generation of a new recommendation automatically, the Compute Image recommendations for cluster task appears in the **Recent tasks** pane. You can observe the progress of the task or cancel it. vCenter Server issues an event when a recommendation generation task starts or ends. If the task fails, vCenter Server issues an alarm of the warning type. In cases of failure, you must check for recommended images for the cluster manually. The recommendation generation task cannot run simultaneously with other vSphere Lifecycle Manager operations, for example remediation and compliance checks. If you need to start another operation immediately, you can cancel the Compute Image recommendations for cluster task at any time.

In ROBO deployments, the automatically triggered recommendation generation is possible only if the local depot and the central vSphere Lifecycle Manager depot are synchronized.

Check for Recommended Images

By using recommended images for your clusters, you ensure that your environment runs the latest verified software. Because the recommendations that vSphere Lifecycle Manager generates for a cluster are not automatically updated when the cluster changes or when new software is available in the vSphere Lifecycle Manager depot, you must periodically perform the check for recommendations task.

- Verify that remediation is not running for the cluster.
- Verify that you have connection to the Internet.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

A recommended image contains updates for your cluster. Recommendations are based on the ESXi versions available in the vSphere Lifecycle Manager depot. When you trigger the check for recommendations task, vSphere Lifecycle Manager first determines the recommended ESXi versions for the cluster. After that, vSphere Lifecycle Manager checks sequentially for newer versions of the vendor add-on, additional components, and firmware add-on that are compatible with the recommended ESXi version and the hardware of the hosts in the cluster. So, sometimes, a recommended image might contain the same ESXi version as the ESXi version in the current image for the cluster but combined with an updated vendor add-on, component, or firmware add-on.

The check for recommendation task is non-cancellable. You must rerun the task periodically to ensure that the recommendations are valid and still suitable to the cluster.

Before you check for recommended images, you must ensure that the cluster is not being remediated. Recommendations generation and remediation are mutually exclusive operations. They cannot run simultaneously.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image** card, click the horizontal ellipsis icon and select **Check for recommended images**.
   When the task finishes, a blue badge appears in the **Image** card.
4. To view the recommended images, click the horizontal ellipsis icon and select **View recommended images**.

vSphere Lifecycle Manager generates recommendations. vSphere Lifecycle Manager might list up to two recommended images applicable to the cluster. Sometimes, no recommended images are available. In such cases, vSphere Lifecycle Manager displays detailed information about why no recommendations are available.
View the recommendations. You can import a recommended image to the cluster and replace the current image that the cluster uses. See Use a Recommended Image.

Use a Recommended Image

For any cluster that you manage with a single image, you can view the images that vSphere Lifecycle Manager recommends and you can replace the current image for the cluster with a recommended image. Using recommended images saves you the time and effort of identifying valid images that are applicable to all hosts in a cluster.

- Check for recommended images for a cluster. See Check for Recommended Images.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image** card, click the horizontal ellipsis icon and select **View recommended images**.
   If the **View recommended images** option is dimmed, no recommended images are available for this cluster.
   Sometimes, even if newer versions of ESXi are available in the vSphere Lifecycle Manager depot, they are not included in a recommended image because of hardware compatibility issues.
   The **Recommended Images** dialog box appears.
4. In the **Recommended Images** dialog box, select a recommended image by clicking the respective radio button and click **Continue**.

Option	Description
Latest in current series	The recommended image is based on the latest ESXi version in the current series of releases. For example, if the ESXi version in your current image is 7.0, this option might include ESXi version 7.0 Update 1 and a related vendor add-on.
Latest and greatest	The recommended image is based on the latest major ESXi version. For example, if the ESXi version in your current image is 7.0, this option might include ESXi version 8.0 and a related vendor addon.

   The selected image is imported to the cluster as a draft. The **Edit Image** card appears.
5. Optional: Edit the image and validate the new image set-up.
6. Click **Save**.
   If you do not save the image, it is saved as a draft. The next time you start editing the image for that cluster, you can use the draft as a starting point.

The recommended image is saved for that cluster. If a draft exists for the cluster, the draft is overriden by the recommended image. No software is installed on the hosts in the cluster at this stage.

To apply the software specification that the image defines, remediate the cluster against the new image. See Run a Remediation Pre-Check for a Cluster and Remediate a Cluster Against a Single Image.

Switching from Using Baselines to Using Images

You can manage a cluster with either baselines or images. You cannot use both at the same time for a single cluster. Even if you do not set up an image for the cluster during cluster creation, you can at any time switch from using baselines to switching images for that cluster.

To switch to vSphere Lifecycle Manager images, you must set up a new image or import an existing one. Before you proceed with setting up or importing an image, vCenter Server checks and reports if the cluster is eligible for using images. For more information about cluster eligibility, see Cluster Eligibility to Use vSphere Lifecycle Manager Images.

With standalone hosts, you can only use baselines. For more information about the difference between baselines and images, see vSphere Lifecycle Manager Baselines and Images.

System Requirements

To switch to using images, the cluster must meet multiple requirements.

- All ESXi hosts in the cluster must be of version 7.0 and later.
- All ESXi hosts in the cluster must be stateful.
  A stateful install is one in which the host boots from a disk.
- No host in the cluster can contain any unknown components.

If a host is of version earlier than 7.0, you must first use an upgrade baseline to upgrade the host and then you can successfully switch to using images. For more information about using baselines for host patching and upgrade operations, see Using vSphere Lifecycle Manager Baselines and Baseline Groups .

For more information about converting a stateless host into a stateful host, find information about Auto Deploy in the *VMware ESXi Installation and Setup* documentation.

Specifics

Several behavioral specifics exist when you switch to using vSphere Lifecycle Manager images.

- If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to a cluster that uses baselines, but you cannot change a cluster that already uses a single image for management purposes.
- When you set up and save an image for a cluster, the image is not applied to the hosts in the cluster unless you remediate the hosts. The mere action of changing the management method does not alter the hosts in the cluster.
- After you set up an image for the cluster and remediate the hosts in the cluster against the image, standalone VIBs are deleted from the hosts.
- After you set up an image for the cluster and remediate the hosts in the cluster against the image, non-integrated solution agents are deleted from the hosts.
- If you enable a solution that cannot work with vSphere Lifecycle Manager, for example Dell EMC VxRail, on an empty cluster and attempt to switch to using an image for that cluster, the transition operation succeeds. However, the result is an unsupported cluster configuration, because both vSphere Lifecycle Manager and the non-integrated solution are enabled on the cluster.

Cluster Eligibility to Use vSphere Lifecycle Manager Images

Switching from baselines to images requires that you set up or import a vSphere Lifecycle Manager image to manage the cluster with. As part of the transition, before you set up the image, vCenter Server triggers an automatic task that checks whether the cluster is eligible to use vSphere Lifecycle Manager images.

The **Check cluster's eligibility to be managed with a single image** task ensures that the cluster is not undergoing remediation against a baseline and checks whether all requirements for using vSphere Lifecycle Manager images are met.

Also, the task checks for standalone VIBs and ensures that no unintegrated solutions are enabled for the cluster. You might not be able to switch to using vSphere Lifecycle Manager images if unintegrated solutions are enabled on the cluster.

Note: If you use any third-party products or solutions, you must confirm with your third-party software vendor whether the respective solution works with vSphere Lifecycle Manager.

The task returns three types of notifications: error, warning, and info.

Errors

The **Check cluster's eligibility to be managed with a single image** task reports an error if the cluster contains at least one host that is not stateful or that is not of a compatible ESXi version, that is 7.0 and later.

Also, the **Check cluster's eligibility to be managed with a single image** returns an error if the cluster contains VIBs of unintegrated solutions. In that case, you must deactivate the unintegrated solution and retry the transition.

Warnings

The **Check cluster's eligibility to be managed with a single image** task issues a warning if the cluster contains at least one host with a standalone VIB or an unknown VIB. Warnings do not block the transition to using vSphere Lifecycle Manager images, but they require special attention or a user action.

For example, you see a warning notification if a host in the cluster contains a standalone VIB, for example a driver, for which a component is available in the vSphere Lifecycle Manager depot. If you want to keep the VIB, you must add the respective component to the vSphere Lifecycle Manager image. Otherwise, the standalone VIB is deleted upon remediation.

You also get a warning if a host in the cluster contains an unknown VIB. Unknown VIBs are standalone VIBs for which no component is available in the vSphere Lifecycle Manager depot. If vSphere Lifecycle Manager detects an unknown VIB, you must import a component that contains the VIB into the vSphere Lifecycle Manager depot and restart the transition. Otherwise, the unknown VIB is deleted upon remediation.

Info

The **Check cluster's eligibility to be managed with a single image** task gives an info notification if the cluster contains at least one host with a standalone VIB, but you can still proceed to setting up a vSphere Lifecycle Manager image for the cluster without any additional actions.

For example, you see an info notification if the cluster is enabled for an integrated solution, for example vSphere HA or vSAN.

Set Up a New Image

To take advantage of all new functionalities that vSphere Lifecycle Manager introduces in vSphere 7.0, you must switch to using vSphere Lifecycle Manager images instead of baselines.

- Verify that all ESXi hosts in the cluster are of version 7.0 and later.
- Verify that all ESXi hosts in the cluster are stateful. A stateful install is one in which the host boots from a disk.
- Verify that all ESXi hosts in the cluster are from the same hardware vendor.
- Verify that no unintegrated solution is enabled for the cluster.

- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to another cluster, which uses baselines, but you cannot change the cluster that already uses a single image.

For conceptual information about vSphere Lifecycle Manager images, see vSphere Lifecycle Manager Images .

For information about how to use vSphere Lifecycle Manager images to manage hosts and cluster, see Using vSphere Lifecycle Manager Images .

1. In the vSphere Client, navigate to a cluster that you manage with baselines and baseline groups.
2. On the **Updates** tab, click **Image**.
3. Click the **Set up image** button.

   vSphere Lifecycle Manager starts checking if the cluster is eligible for using images. If no problems are reported, the **Convert to an Image** pane appears.

4. If the **Check cluster's eligibility to be managed with a single image** tasks reports an error or a warning that requires an action, resolve the issue and restart the procedure.
5. From the **ESXi Version** drop-down menu, select an ESXi image.
6. Optional: Add a vendor add-on to the image.
   a) Click **Select**.
      The **Select Vendor Addon** appears.
   b) Select an add-on from the list.
      An information panel appears on the right. The information panel shows information about the components that the add-on adds to the ESXi image and the components that it removes from the image.
   c) From the **Version** drop-down menu for the selected add-on, select the add-on version.
   d) Click **Select**.
7. Optional: Add a firmware and drivers add-on to the image.
   a) Click **Select**.
      The **Select Firmware and Drivers Addon** appears.
   b) Select a hardware support manager from the respective drop-down menu.
      A list of firmware and drivers add-ons appears.
   c) Select an add-on from the list.
      An information panel appears on the right. The information panel shows information about the supported ESXi versions and whether the add-on contains a driver or not.
   d) From the **Version** drop-down menu for the selected add-on, select the add-on version.
   e) Click **Select**.
8. Optional: Add additional components to the image.
   a) Click **Show details**.
   b) Click **Add components**.
      The **Add Components** dialog box appears.
   c) Optional: Use the **Show** drop-down menu to sift out the components that are not part of the selected vendor add-on.
   d) Select one or multiple components from the list.
      An information panel appears on the right. The information panel shows information about the component that you selected first.
   e) From the **Version** drop-down menu for the selected component, select the component version.
   f) Click **Select**.
      The selected components appear in the list of components that the image contains. You can use the **Show** drop-down menu to sift out the additional components.
   g) Optional: Click **Hide details** to hide the list of components.
9. Optional: To validate the image, click the **Validate** button.
   You validate an image to check for missing dependencies and component conflicts.
10. Click **Save**.
    Saving the image triggers an automatic compliance check. All hosts in the cluster are checked against the image.

11. In the **Convert to an Image** pane, finish the image setup.
    a) Click the **Finish image setup** button.
    b) In the **Finish image setup** dialog box, click **Yes, finish image setup**.

You set up an image for the cluster. You now manage all hosts in the cluster collectively with a single image for the cluster. Upon remediation, the image is installed on all hosts in the cluster.

To apply the image to all hosts in the cluster, remediate the cluster against the image.

Import an Existing Image

To take advantage of all new functionalities that vSphere Lifecycle Manager introduces in vSphere 7.0, you must switch to using vSphere Lifecycle Manager images instead of baselines.

- Verify that all ESXi hosts in the cluster are of version 7.0 and later.
- Verify that all ESXi hosts in the cluster are stateful. A stateful install is one in which the host boots from a disk.
- Verify that all ESXi hosts in the cluster are from the same hardware vendor.
- Verify that no unintegrated solution is enabled for the cluster.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to another cluster, which uses baselines, but you cannot change the cluster that already uses a single image.

For conceptual information about vSphere Lifecycle Manager images, see vSphere Lifecycle Manager Images .

For information about how to use vSphere Lifecycle Manager images to manage hosts and clusters, see Using vSphere Lifecycle Manager Images .

1. In the vSphere Client, navigate to a cluster that you manage with baselines and baseline groups.
2. On the **Updates** tab, click **Image**.
3. Click the **Import Image** button.
   The **Import Image** dialog box appears.
4. Select a JSON file to import and click **Next**.
   - Click the **Browse** button and select a JSON file on your local machine.
   - Enter a valid URL to a JSON file on a remote web server.

   vSphere Lifecycle Manager starts checking if the cluster is eligible for using images. If no problems are reported, the **Convert to an Image** pane appears. The elements of the imported image appear in the **Define Image** card.
5. Optional: Customize the imported image by changing any of its elements.
6. Optional: To validate the image, click the **Validate** button.
   You validate an image to check for missing dependencies and component conflicts.
7. Click **Save**.
   Saving the image triggers an automatic compliance check. All hosts in the cluster are checked against the image.
8. In the **Convert to an Image** pane, finish the image setup.
   a) Click the **Finish image setup** button.
   b) In the **Finish image setup** dialog box, click **Yes, finish image setup**.

You now manage all hosts in the cluster collectively with a single image for the cluster. Upon remediation, the image is installed on all hosts in the cluster.
To apply the image to all hosts in the cluster, remediate the cluster against the image.

Firmware Updates

You can use vSphere Lifecycle Manager images to perform firmware updates on the ESXi hosts in a cluster. Using vSphere Lifecycle Manager images simplifies the host update operation. With a single operation, you update both the software and the firmware on the host.

In earlier vSphere releases, you could perform firmware updates on vSAN clusters by using system-managed baselines. For non- vSAN clusters, firmware updates had to be manual.

Starting with vSphere 7.0, you can easily update the firmware in any cluster that you manage with a single image. Firmware updates are not available for clusters that you manage with baselines.

To apply firmware updates to the hosts in a cluster that you manage with a single image, you must include a special type of add-on, the firmware and drivers add-on, in the image and remediate the cluster to apply the image to all hosts. The firmware and drivers add-on is a vendor-provided add-on that contains the components that encapsulate firmware update packages. The firmware and drivers add-on might also contain the necessary drivers.

Unlike vendor add-ons, firmware and drivers add-ons are not distributed through the official VMware online depot or as offline bundles available at my.vmware.com. For a given hardware vendor, firmware updates are available in a special vendor depot, whose content you access through a software module called a hardware support manager. The hardware support manager is a plug-in that registers itself as a vCenter Server extension. Each hardware vendor provides and manages a separate hardware support manager that integrates with vSphere. For each cluster that you manage with a single image, you select the hardware support manager that provides the firmware updates for the cluster. After you determine the hardware support manager that you want to use for a cluster, the hardware support manager provides you with a list of the available firmware updates. When you select and include a firmware add-on to an image, that add-on might modify the specified image by adding or removing components. The firmware add-on also defines the firmware versions to be installed on the hosts. During remediation, vSphere Lifecycle Manager applies the image to the hosts and requests the selected hardware support manager to update the firmware on the hosts in accordance with the firmware add-on specified in the image.

Selecting a hardware support manager and including a firmware add-on in your image guarantees that during a compliance check, vSphere Lifecycle Manager also determines the firmware compliance for the cluster. So, you can easily detect and remediate any unwanted drifts. The hardware support manager is also responsible for retrieving the firmware versions on the host hardware, and, in some cases, determining the appropriate drivers for the updated firmware version.

For vSAN clusters, the hardware support manager inspects the hosts in the cluster to determine their current I/O device controllers and firmware. During a hardware compatibility check for the cluster, vSphere Lifecycle Manager checks whether the firmware in the image is compatible with the hardware in the cluster as per vSAN Hardware Compatibility List (vSAN HCL). The hardware compatibility check ensures that when vSphere Lifecycle Manager remediates the cluster and applies the image to all hosts, the firmware and drivers on the hosts are certified for use with vSAN.

Deploying Hardware Support Managers

The deployment method and the management of a hardware support manager plug-in are determined by the respective OEM.

Several of the major OEMs develop and supply hardware support managers. For example:

- Dell
  The hardware support manager that Dell provides is part of their host management solution, OpenManage Integration for VMware vCenter (OMIVV), which you deploy as an appliance.
- HPE
  The hardware support managers that HPE provides are part of their management tools, iLO Amplifier and OneView, which you deploy as appliances.
- Lenovo
  The hardware support manager that Lenovo provides is part of their server management solution, Lenovo XClarity Integrator for VMware vCenter, which you deploy as an appliance.

- Hitachi
  The hardware support manager that Hitachi provides, Hitachi Unified Compute Platform Advisor, is infrastructure automation and management software for all Hitachi converged, hyperconverged, and integrated systems, which you deploy as an appliance.
- Cisco
  The hardware support manager that Cisco provides is integrated with Cisco Intersight Infrastructure Service, which is part of Cisco Intersight and you activate the hardware support manager from within the Cisco Intersight SaaS-based management platform. No additional appliances are required on your vCenter Server instance.

You can find the full list of all VMware-certified hardware support managers in the VMware Compatibility Guide at https://www.vmware.com/resources/compatibility/search.php?deviceCategory=hsm.

Deploying and Configuring Hardware Support Managers

Regardless of the hardware vendor, you must deploy the hardware support manager appliance on a host with sufficient memory, storage, and processing resources. Typically, hardware support manager appliances are distributed as OVF or OVA templates. You can deploy them on any host in any vCenter Server instance.

Note: If vCenter Server is configured with a proxy for internet access, the proxy must be able to reach any hardware support manager registered with that vCenter Server instance. You must either assign the hardware support manager a private IP address within the `10.x.x.x` range, which is automatically exempt from proxy use, or enable a direct access to the registered hardware support manager by configuring the proxy settings with an exception for its IP address.

After you deploy the appliance, you must power on the appliance virtual machine and register the appliance as a vCenter Server extension. You might need to log in to the appliance as an administrator. Each hardware support manager might register with only one or multiple vCenter Server systems.

A vCenter Server plug-in user interface might become available in the vSphere Client after you deploy a hardware support manager appliance, but the hardware support manager might also have a separate user interface of its own. For example, OMIVV, iLO Amplifier, and Lenovo XClarity Integrator for VMware vCenter all have a vCenter Server plug-in user interface, which helps you configure and work with the respective hardware support manager.

Each hardware support manager has its own mechanism of managing the actual firmware packages and making firmware add-ons available for you to choose.

The successful integration between the hardware support manager and vSphere Lifecycle Manager might require a specific configuration of the hardware support manager. For example, with OMIVV, you must first create a connection profile. Then, you must create a cluster profile and associate it with a cluster before you can add a firmware add-on from Dell to the image for that cluster.

For detailed information about deploying, configuring, and managing hardware support managers, refer to the respective OEM-provided documentation.

Use an Image for Firmware Updates

vSphere Lifecycle Manager allows you to manage the firmware lifecycle on ESXi hosts that are part of a cluster that you manage with a single image.

- Deploy the vendor-provided hardware support manager and register it as a vCenter Server extension. For more information about deploying and managing a hardware support manager, see the respective OEM documentation.
- If you use the hardware support manager provided by Dell, create a cluster profile and associate it with the cluster. For more information , review the OpenManage Integration for VMware vCenter (OMIVV) documentation.
- Verify that all hosts in the cluster are from the same vendor.

- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Image**.
3. In the **Image** card, click the **Edit** button.
4. In the **Edit Image** card, for the **Firmware and Drivers Addon**, click **Select**.
   The **Firmware and Drivers Addon** dialog box appears.
5. In the **Firmware and Drivers Addon** dialog box, select a hardware support manager from the drop-down menu.
   The selected hardware support manager must be from the same hardware vendor as the hosts in the cluster. Otherwise, during a compliance check, the hardware support manager reports the selected firmware and drivers add-on to be incompatible with the host or hosts that are from a different vendor. Firmware remediation fails.
   A list of all available firmware add-ons appears.
6. Select a firmware add-on from the list.
   An information panel appears on the right. The panel contains information about the supported ESXi versions and whether the selected add-on contains the necessary drivers.
7. Click **Select**.
   The selected firmware and drivers add-on is included in the image.
8. In the **Image** card, validate and save the image.
   After the image is saved, a compliance check against the new image is triggered for the cluster.
9. In the **Image Compliance** card, review the compliance check results for the cluster and for each host.
10. If any host in the cluster has firmware that is non-compliant with the new image firmware, remediate the respective host or the cluster.
    a) Optional: In the **Image Compliance** card, run a remediation pre-check to ensure that remediation finishes successfully.
       - To run a pre-check for all hosts in the cluster, click the **Run Pre-check** button.
       - To run a pre-check for a single host, click the vertical ellipsis icon for the host and select **Run Pre-check**.

    b) In the **Image Compliance** card, initiate remediation.
       - To remediate all hosts in the cluster, click the **Remediate All** button.
         During cluster remediation, if the remediation of a single host fails, the remediation for the cluster ends prematurely.
       - To remediate a single host, click the vertical ellipsis icon for the host and select **Remediate**.

    You are not obliged to start remediation immediately after setting up an image for a cluster. However, nothing is installed on the hosts unless you remediate them against the image for the cluster. The firmware on the hosts is actually updated only after successful remediation. You can remediate the objects in your environment at any time that is convenient for you.

The firmware on the hosts in the cluster is updated to the firmware version specified in the firmware add-on for the image.

Hardware Compatibility Checks

vSphere Lifecycle Manager automates the process of validating the hardware compliance of hosts and clusters against a selected ESXi version. Hardware compatibility checks ensure that the host or cluster hardware is compliant with the VMware Compatibility Guide (VCG) and vSAN Hardware Compatibility List (vSAN HCL).

Hardware Compatibility Lists

Hardware compatibility lists are lists of hardware certified for use with various vSphere releases. The VCG contains information about server models and I/O devices that are certified for use with particular vSphere releases. Besides VCG, vSAN maintains a separate hardware compatibility list that lists all I/O device controller hardware and the respective firmware versions certified for use with vSAN. The vSAN HCL also contains information about the disk drives that a specific vSphere release supports and the earliest disk drive firmware version certified for use with vSAN.

With vSphere Lifecycle Manager, you can perform the following tasks.

- Check the hardware compatibility of a single host.
- Check the hardware compatibility of a vSAN cluster.

In general, hardware incompatibilities do not prevent remediation and are not resolved upon remediation. However, you can configure vSphere Lifecycle Manager to prevent remediation when hardware compatibility issues exist for a cluster. For information about configuring the global vSphere Lifecycle Manager remediation settings, see Configure Remediation Settings for vSphere Lifecycle Manager Images . For information about configuring the remediation settings for a particular cluster, see Edit the Remediation Settings for a Cluster.

Cluster-Level Hardware Compatibility Checks

Running a hardware compatibility check on your clusters before remediating them helps you ensure good vSAN cluster health and avoid entering into unsupported and unwanted configurations after remediation.

Cluster-level hardware compatibility checks are available only for vSAN clusters that you manage with a single image. If a vSAN cluster uses baselines, hardware compatibility checks are not available. Also, if a cluster uses a single vSphere Lifecycle Manager image but vSAN is not enabled for that cluster, hardware compatibility checks for that cluster are not available. The hardware compatibility checks for vSAN clusters are performed against the vSAN HCL.

Note: To perform a hardware compatibility check for a vSAN cluster, the vSAN HCL data that is available to vSphere Lifecycle Manager must be up to date. vSAN HCL data is synchronized automatically or manually, in environments without connection to the Internet. For more information about maintaining the vSAN HCL data up-to-date, see the vSAN documentation.

When you initiate a hardware compatibility check for a cluster, vSphere Lifecycle Manager scans the image and verifies that all elements of the image are compatible with the cluster hardware. vSphere Lifecycle Manager validates only those hardware devices that vSAN uses. Because cluster-level hardware compatibility checks validate the compatibility between the cluster hardware and the cluster image, the compatibility results might not be accurate unless the cluster is successfully remediated and the image is applied to all hosts in the cluster.

Hardware compatibility issues are reported as warnings, but they do not prevent you from remediating the hosts in the cluster against the image.

During a hardware compatibility check for a cluster, vSphere Lifecycle Manager performs the following tasks:

- Verifies that all storage device drivers are certified for use with the ESXi version specified in the image.
- Verifies that the image contains the correct storage device driver and firmware versions as per vSAN HCL.
- Suggests a compatible storage device driver version for the cluster as per vSAN HCL.
- Verifies that all disk drives in the cluster are certified for use with the ESXi version specified in the image as per vSAN HCL.
- Verifies that the physical disk drives behind RAID-0 logical volumes are certified for use with the ESXi version specified in the image as per vSAN HCL.
- Verifies that the disk drive firmware version specified in the image for the cluster is equal to or higher than the earliest supported firmware version as per vSAN HCL.
- Verifies that the target firmware version for the physical drives behind RAID-0 logical volumes is equal to or higher than the earliest supported firmware version as per vSAN HCL.

Note: vSphere Lifecycle Manager performs the full driver and firmware verification only if you configure vSphere Lifecycle Manager with a hardware support manager and add a firmware add-on to the vSphere Lifecycle Manager image. Without using a hardware support manager, vSphere Lifecycle Manager only validates the PCI device and driver versions and the disk drive version.

Disk Drive Validation

During a cluster-level hardware compatibility check, vSphere Lifecycle Manager verifies that the disk drives that vSAN uses are supported and certified as per the vSAN Hardware Compatibility List (HCL). vSphere Lifecycle Manager also ensures that the disk drive firmware version specified in the cluster image is compatible with the cluster hardware.

The disk drives in a vSAN cluster and the firmware installed on the drives are of paramount importance for the overall vSAN cluster health. For example, a faulty disk drive firmware might cause performance issues and unexpected vSAN input-output behavior. You can use vSphere Lifecycle Manager hardware support managers to perform disk drive firmware upgrades. Before you upgrade the disk drive firmware, however, you must ensure that the target firmware version is supported as per the vSAN HCL.

Note: For each device, the vSAN HCL lists the earliest supported firmware version. All firmware versions later than the specified in the vSAN HCL are supported.

Supported Disk Drives Types

vSphere Lifecycle Manager validates the following types of disk drives and storage device configurations:

- HDD (SAS/SATA)
- SSD (SAS/SATA)
- SAS/SATA disk drives behind single-disk RAID-0 logical volumes

System Requirements for Disk Drive Validation

- vCenter Server 7.0 Update 3 and later
- ESXi 7.0 and later

RAID-0 Logical Volumes

vSphere Lifecycle Manager can validate the physical SAS/SATA disk drives behind single-disk RAID-0 logical volumes. The following requirements exist:

- The RAID controller is in a RAID or mixed mode.
  For more information about the RAID and mixed mode, see the VMware knowledge base article at https://kb.vmware.com/s/article/53573.
- vCenter Server 7.0 Update 3 and later
- ESXi 7.0 and later
- The hardware support manager must be upgraded and certified to work with vSphere 7.0 Update 3.
  If the you do not use an upgraded version of the hardware support manager, the compliance status of the physical drives behind RAID-0 logical volumes is unknown. In this case, you must manually validate the disk drives and the target firmware version and override the compliance status for those disks.

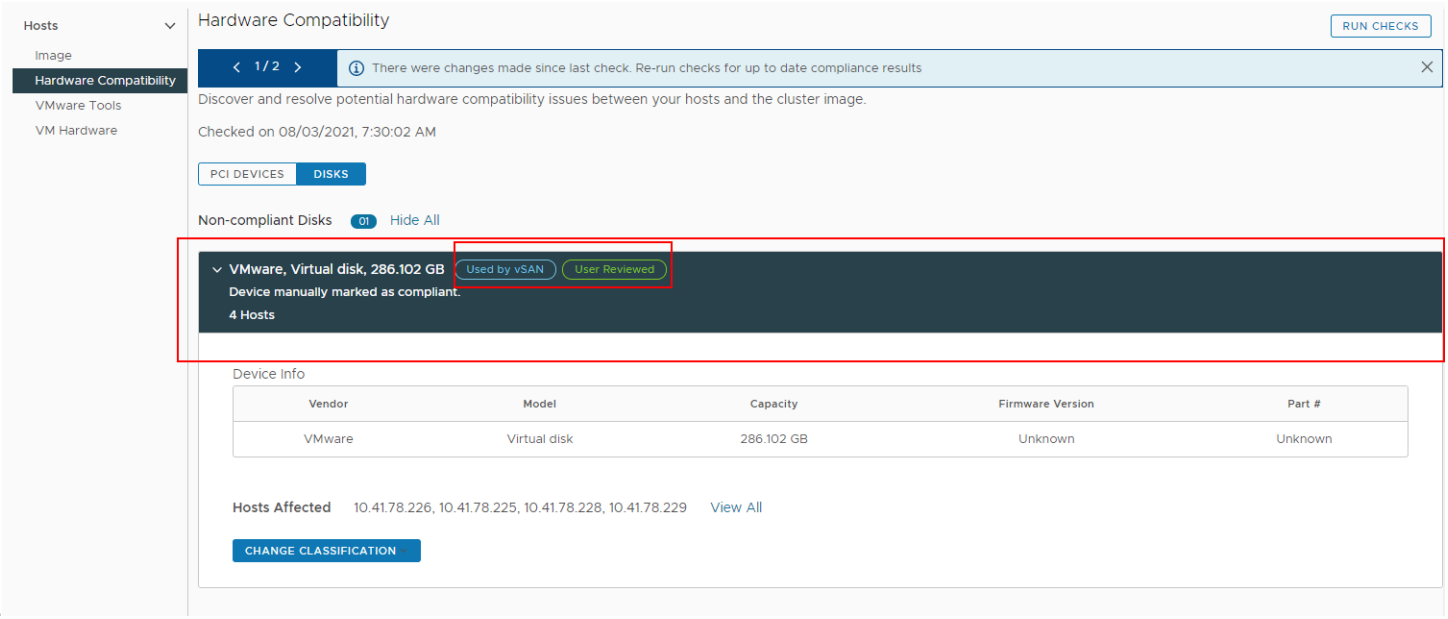
Disk Drive Validation Results

vSphere Lifecycle Manager does not display a disk drive compatibility status and compatibility information for every single disk in the vSAN disk group. vSphere Lifecycle Manager groups the disk drives that vSAN uses by vendor, model, target firmware version, capacity, and part number. That is, all disk drives by the same vendor, the same model, and with the same target firmware version form one entry in the list of disk devices.

Disk drives can be compliant or non-compliant. In the cases when vSphere Lifecycle Manager cannot find a unique match for a disk device in the vSAN HCL, vSphere Lifecycle Manager prompts you to manually specify the exact device that you want to validate. vSphere Lifecycle Manager then calculates the compliance status based on your selection.

When vSphere Lifecycle Manager is unable to determine the disk drive compliance, the respective devices are listed as non-compliant. You can manually validate those devices and set the compliance status to compliant or non-compliant.

For each entry in the disk device list, you can view summarized information about the disk, the compliance status, the number of affected hosts, and a label that shows whether the compliance status is manually set or whether the device is certified. The **Used by vSAN** label is attached to all disk devices used by vSAN.



If you expand the entry, you can view detailed compliance information about the respective disk device and the affected hosts.

When a new disk is added to a vSAN cluster, you must manually re-run the check to obtain the new compliance information about the cluster. Similarly, if you remove a disk from the vSAN disk group, you must re-run the hardware compatibility check to obtain an updated compliance information about the cluster.

Check the Hardware Compatibility of a Cluster

For a vSAN cluster that you manage with a single image, you can check the compliance between the image components and the hardware in the cluster. The check is performed against the vSAN Hardware Compatibility List (vSAN HCL) and ensures that if the image is applied to the hosts, the result after remediation is in accordance with the vSAN HCL.

- Verify that vSAN is enabled for the cluster.
- Verify that the cluster uses a single image.
- Verify that all hosts in the cluster are from the same vendor.
- To validate the compatibility between the PCI device and disk device hardware and target firmware version, verify that the image for the cluster includes a firmware add-on.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a vSAN cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Hardware Compatibility**.
   In the **Hardware Compatibility** pane, you see the results from the previous compatibility check.

3. In the **Hardware Compatibility** pane, click the **Run Checks** button.

vSphere Lifecycle Manager displays all compatibility information and issues in the **Hardware Compatibility** pane. You can see detailed compatibility information for each PCI device or disk drive.
Review the result from the hardware compatibility check.

Resolve any issues before you remediate the cluster.

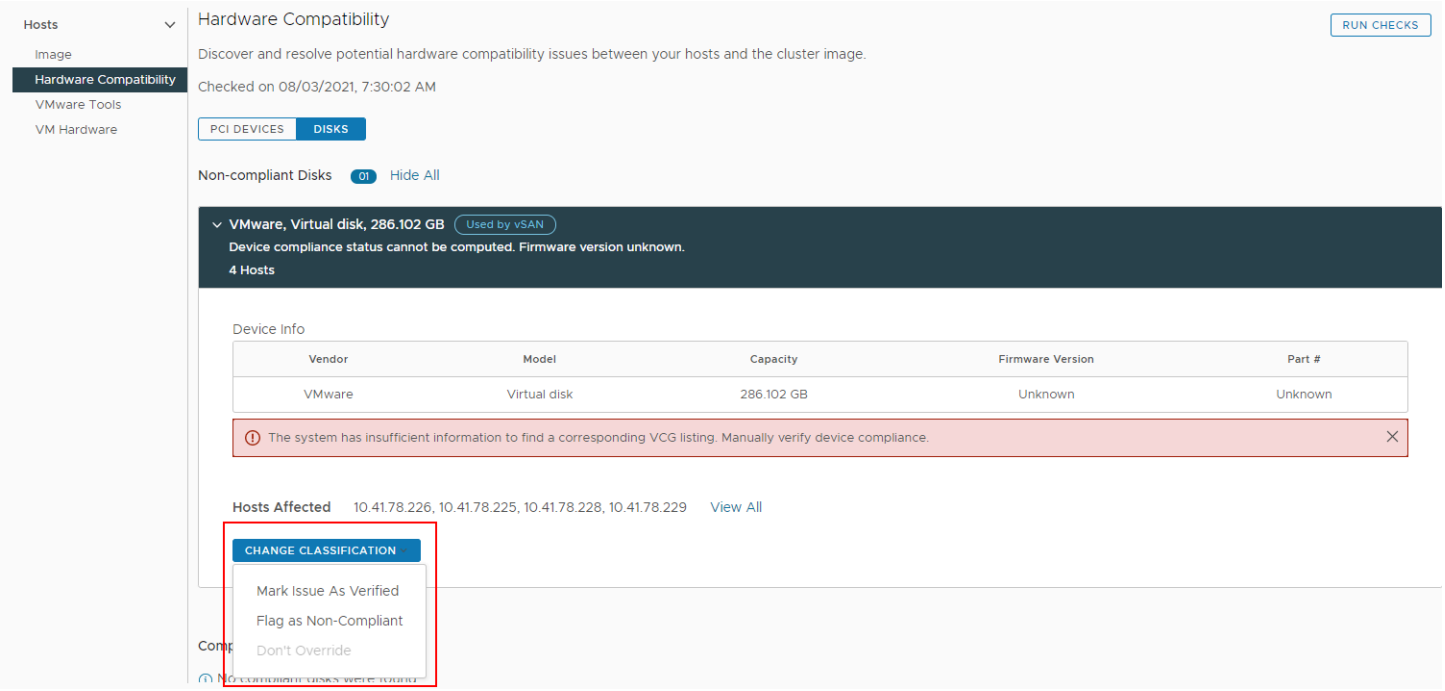
Change the Compliance Status of a Disk Device Manually

You can manually change the compliance status of a disk device and mark it as compliant or non-compliant.

- vCenter Server 7.0 Update 3
- Verify that vSAN is enabled for the cluster.
- Verify that the cluster uses a single image.
- Verify that all hosts in the cluster are from the same vendor.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

In cases when the compliance status of a disk drive is unavailable, you must perform the hardware compatibility check manually and mark the device as compliant or non-compliant.

1. In the vSphere Client, navigate to a vSAN cluster that you manage with a single image.
2. On the **Updates** tab, select **Hosts** > **Hardware Compatibility**.
   In the **Hardware Compatibility** pane, you see the results from the previous compatibility check.
3. Click the **Disks** button.
   You see a list of all non-compliant and compliant disk devices.
4. Click the disk device whose compliance status you want to override.
5. Click the **Change Classification** button.
   A drop-down menu appears.



6. Select the compliance status to apply to the disk device.
   - To mark the issue as compliant, select **Mark Issue As Verified**.
   - To mark the issue as non-compliant, select **Flag as Non-Compliant**.

   The **Mark Issue As Verified** option is not available for compliant devices. The **Flag as Non-Compliant** option is unavailable if the disk device is non-compliant
7. Optional: To undo the override selection, select **Don't Override** from the **Change Classification** drop-down menu.

You changed the compliance status of a disk device. However, the disk device remains in its original list until you run a new hardware compatibility check.

If you marked the device as verified, a **User Reviewed** label appears for the disk group.

If you marked the device as non-compliant, a **Flagged** label appears for the disk group.

Run a new hardware compatibility check so that the new compliance status for a disk is saved.

Automatically Triggered Hardware Compatibility Checks for vSAN Clusters

Starting with vSphere 7.0 Update 1, vSphere Lifecycle Manager performs regular hardware compatibility checks for the vSAN clusters that you manage with a single image. In addition, certain vSphere Lifecycle Manager operations also trigger an automatic hardware compatibility check. Automated hardware compatibility checks are available for vSAN clusters that use a single image.

For information about hardware compatibility checks and instructions how to manually perform a hardware compatibility check for a cluster or for a single host, see Hardware Compatibility Checks.

vSphere Lifecycle Manager Operations That Trigger a Hardware Compatibility Check

vSphere Lifecycle Manager performs an automatic hardware compatibility check for any vSAN cluster that you manage with a single image in the following cases.

- You edit the image for the cluster and save the image.
  When you edit and save an image, vSphere Lifecycle Manager starts the Check hardware compatibility of cluster's host with image task even for clusters without vSAN. In such case, vSphere Lifecycle Manager only returns a warning that image hardware compatibility is not verified in non- vSAN clusters.
  If the automatically triggered hardware compatibility task fails, you can still save the new image for the cluster.
- You initiate a remediation pre-check or remediation.
  The hardware compatibility check is a part of the remediation pre-check and remediation task for vSAN clusters. If a cluster is not vSAN-enabled, vSphere Lifecycle Manager does not perform a hardware compatibility check when you initiate a remediation pre-check or remediation.
  You can configure how vSphere Lifecycle Manager behaves in case of hardware compatibility issues.
- You add or remove a host to and from the cluster.
  When you add or remove a host to and from the cluster, vSphere Lifecycle Manager invalidates the hardware compatibility check results for the cluster and issues a warning. You must rerun a hardware compatibility check to obtain valid information about potential hardware compatibility issues. Alternatively, you can remediate the cluster or run a remediation pre-check, which both automatically trigger a hardware compatibility check.

Regular Hardware Compatibility Checks

The vSAN Hardware Compatibility List (vSAN HCL) database changes regularly. For example, when VMware certifies new OEM devices, drivers, or firmware, those become part of the vSAN HCL database. Similarly, devices, drivers, or firmware that are not supported anymore are removed from the vSAN HCL database.

Changes in the vSAN HCL database might make your hardware compatibility results invalid and outdated. To provide you with valid hardware compatibility information, vSphere Lifecycle Manager runs a periodic hardware compatibility check against the latest vSAN HCL data.

The periodic hardware compatibility check is a preconfigured scheduled task that you can edit and force to run at any time. By default, the task runs every 24 hours. The scheduled task is configured at a vCenter Server level. If a vCenter Server system contains no vSAN clusters that you manage with a single image, vSphere Lifecycle Manager skips the scheduled hardware compatibility check. This periodic task runs only for vSAN clusters that you manage with a single image.

Host-Level Hardware Compatibility Checks

You can run a hardware compatibility check for any host to determine which ESXi version the host hardware is compatible with. The hardware compatibility check ensures that the host hardware, that is server model and I/O devices, is certified for use with a selected ESXi version.

The hardware compatibility check for a host is performed against the VCG, unless the host is in a vSAN cluster. If the host is in a vSAN cluster, the hardware compatibility of the I/O devices that are used by vSAN is checked against the vSAN HCL. All other I/O devices are checked against the VCG.

You can check the hardware compatibility of any host, whether it is in a cluster that uses a single image or baselines. You can also check the hardware compatibility of a standalone host.

After the hardware compatibility check, vSphere Lifecycle Manager shows the compliance status for the server and hardware devices. The server and devices might have one of the three different states: compatible, incompatible, and unknown. For more information about compatibility statuses, see Hardware Compatibility Report for a Host.

If the server status is incompatible, vSphere Lifecycle Manager does not proceed with checking the compatibility for the hardware devices.

Check the Hardware Compatibility of a Host

You can check the hardware compatibility of a host to determine whether the host hardware is certified for use with a selected ESXi version. The hardware compatibility check is performed against the VMware Compatibility Guide (VCG) or, if the host is in a vSAN cluster, against the vSAN Hardware Compatibility List (HCL)

- If needed, synchronize hardware compatibility data. See Sync Hardware Compatibility Data.
- Verify that the Customer Experience Improvement Program is enabled.
- Verify that vCenter Server is connected to the Internet.
- Verify that the host is not part of an VxRail environment.

- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

1. In the vSphere Client, navigate to a standalone host or a host in a cluster.
2. On the **Updates** tab, select **Hosts** > **Hardware Compatibility**.
3. In the **Hardware Compatibility** pane, select your task.
   - To run a hardware compatibility check for the host for the first time, select a target ESXi from the drop-down menu and click **Apply**.
   - To check the hardware compatibility between the host and the already selected target ESXi version, click **Re-run Checks**.
   - To choose a new target ESXi version for the hardware compatibility check, click **Edit** and select a new target ESXi version.
   - To export the hardware compatibility report in a CSV format, click the **Export** button.

vSphere Lifecycle Manager displays the result from the compatibility check. You can see a list of the compatible, incompatible, and unknown devices. For each device, you can see full details by clicking the expand button.

Hardware Compatibility Report for a Host

The hardware compatibility report gives you information whether for a selected server model and hardware devices, vSphere Lifecycle Manager finds records for a target ESXi version in the VMware Compatibility Guide (VCG).

Server Hardware Compatibility

Host Model is Not Compatible	This compatibility status indicates that there are no records for the selected ESXi version in the VCG. If the host is not compatible with the selected ESXi version, vSphere Lifecycle Manager does not proceed to checking the compatibility of the devices. In the **Host Model Compatibility** card, you can see details about the host: server model name, CPU model, and the BIOS version running on the host. At the bottom of the card, you see a list of all certified CPU series for the target ESXi version.
Host Model is Compatible	This compatibility status indicates that the host is certified for use with the selected ESXi version as per VCG. When the host is compatible, vSphere Lifecycle Manager proceeds with the device validation. In the **Host Model Compatibility** card, you can see details about the host: server model name, CPU model, and the BIOS version running on the host. Because in VCG the information about CPUs is based on CPU series, and not specific models, you might need to manually check if the CPU of the host is part of the supported CPU series. You might also need to manually check if the BIOS version on the host matches any of the compatible BIOS versions for the CPU series as per VCG.
Hardware Compatibility Checks Not Supported for the Host Vendor Model	When the server model is not part of the list of certified OEMs, vSphere Lifecycle Manager does not perform a hardware compatibility check and you do not see a hardware compatibility report for the selected host.

Device Hardware Compatibility

The compatibility statuses for devices are: compatible, incompatible, and unknown.

Unknown	Unknown devices are devices for which no records exist in VCG. When you click the expand button for the device, you see the following device information: device IDs, driver and firmware currently running on the device. No compatibility data is generated and displayed. The unknown status might also indicate that multiple matches exist in the VCG for the respective device. In such cases, use the device ID to manually check if the hardware device matches any of the supported devices for the target ESXi version in the VCG.
Incompatible	The incompatible status indicates that no records exist in the VCG for the selected ESXi version. When you click the expand button for the device, you see information about the ESXi versions that are compatible with the device as per VCG.
Compatible	The compatible status indicates that the device is compatible with the selected ESXi version as per VCG. When you click the expand button for the device, you see the following device information: device IDs, driver and firmware currently running on the device. For compatible devices, you might need to manually confirm that the driver-firmware combination running on the device is supported as per VCG.

Sync Hardware Compatibility Data

To initiate a hardware compatibility check for a host, the hardware compatibility data from VMware Compatibility Guide (VCG) must become available to vSphere Lifecycle Manager.

Verify that vCenter Server can access the following sites:

- vvs.esp.vmware.com
- auth.esp.vmware.com

Synchronizing compatibility ensures that the compatibility information from VCG becomes available to vSphere Lifecycle Manager. The synchronization task is not automated. When no compatibility data is available for use to vSphere Lifecycle Manager, you must trigger the compatibility data synchronization manually.

vSAN HCL data is not updated through synchronization. If you want to check the hardware compatibility of a host that is in a vSAN cluster, you must first verify that vSAN HCL data is up to date. For more information about updating vSAN HCL data, see the vSAN documentation.

1. In the vSphere Client, navigate to a standalone host or a host in a cluster.
2. On the **Updates** tab, select **Hosts** > **Hardware Compatibility**.
3. In the **Hardware Compatibility** pane, click **Sync compatibility data**.
4. In the **Sync hardware compatibility data** dialog box, click **Go to Lifecycle Manager**.
   You are redirected to the vSphere Lifecycle Manager home view.
5. Select **Actions** > **Sync HCL**.
   The Update HCL data task appears in the **Recent Taks** pane.

After the Update HCL data task finishes, the compatibility data from the VCG becomes available to vSphere Lifecycle Manager.

Check the hardware compatibility of your hosts against VCG before you update or upgrade them to a later ESXi version.

vSphere Lifecycle Manager Images and Other VMware Products and Solutions

You can use a vSphere Lifecycle Manager image to manage a cluster if the cluster only contains solutions integrated to work with vSphere Lifecycle Manager. If an unitegrated solution is enabled on a cluster, you cannot use vSphere Lifecycle Manager images to manage that cluster, but you can still use baselines and baseline groups.

A solution is a VMware product that integrates with vCenter Server and adds some new functionality to the ESXi hosts in the inventory.

When you enable a solution for a cluster that uses a vSphere Lifecycle Manager image, the solution automatically uploads an offline bundle with components into the vSphere Lifecycle Manager depot and adds its component to all hosts in the cluster. You cannot control the lifecycle of solution components. For example, if you export the image, solution components are not part of the exported image.

Integrated Solutions

You can manage a cluster with a single image if the cluster has any of the following solutions enabled.

- vSphere High Availability
- vSAN
  For more information about the integration between vSAN and vSphere Lifecycle Manager, see vSAN Clusters and vSphere Lifecycle Manager and the *Administering VMware vSAN* documentation.
- vSAN File Services
- vSphere with Tanzu
  For detailed information about the integration between vSphere with Tanzu and vSphere Lifecycle Manager, see the documentation.
- VMware NSX-T Data Center™
  For more information about the integration between VMware NSX-T Data Center™ and vSphere Lifecycle Manager, see the *NSX-T Data Center Administration* documentation.
- VMware Cloud Foundation
  vSphere Lifecycle Manager is available as an option in the VMware Cloud Foundation Workload Domain. For more information, see the *VMware Cloud Foundation Lifecycle Management* documentation.

You can also use baselines for clusters that have those solutions enabled.

Unintegrated Solutions

You cannot manage a cluster with a single image if the cluster has any of the following solutions enabled.

- VMware NSX® Data Center for vSphere®
- VMware vSphere Replication
- Dell EMC VxRail

You can use baselines and baseline groups to manage clusters that have those solutions enabled.

vSAN Clusters and vSphere Lifecycle Manager

You can manage a vSAN cluster by using vSphere Lifecycle Manager baselines and baseline groups or by using a single image for that cluster. Working with vSAN clusters has its specifics regardless of whether you manage the cluster with a single image or with baselines.

Managing a vSAN Cluster by Using Recommendation Baseline Groups

You can update and upgrade the hosts in a vSAN cluster by using automatically generated system-managed baselines groups. Those system-managed baseline groups are called recommendation baseline groups. Recommendation baseline groups do not contain firmware and driver updates. Recommendation baselines contain only patch or upgrade baselines.

If you want to switch to using images for a vSAN cluster that contains ESXi hosts of versions earlier than 7.0, you must first use an upgrade baseline to upgrade the hosts. Then, you can switch to using a vSphere Lifecycle Manager image for the cluster.

For more information about recommendation baselines, see About Recommendation Baseline Groups.

For more information about using baselines to manage hosts and clusters, see Using vSphere Lifecycle Manager Baselines and Baseline Groups .

Managing a vSAN Cluster with a Single Image

The image that you use for a cluster defines the full software stack to run on the hosts in that cluster: ESXi version, vendor customization, drivers, and firmware. When you manage a vSAN cluster with a single image, you can take advantage of the functionalities that vSphere Lifecycle Manager images provide.

- You can update the firmware on all hosts in the vSAN cluster.
  You perform firmware update by setting up an image that contains a firmware add-on and remediating the vSAN cluster against that image. For more information about performing firmware updates by using vSphere Lifecycle Manager images, see Firmware Updates.
- You can run a hardware compatibility check for the cluster.
  The hardware compatibility check task verifies that the image for the cluster can be successfully applied to all hosts and that it is compliant with the vSAN Hardware Compatibility List (HCL). For more information about hardware compatibility checks, see Hardware Compatibility Checks.
- You can check firmware compliance with the image.
  When you perform a compliance check against the image for a cluster, firmware compliance is also checked. As a result, you can easily notice if a driver or firmware in your cluster becomes non-compliant. For more information about checking the compliance of a cluster against an image, see Checking Compliance Against a Single Image.
- You can use vSphere Lifecycle Manager recommended images.
  When you manage a vSAN cluster with vSphere Lifecycle Manager images, the vSAN recommendation engine does not generate vSAN health alarms or recommendation baselines for that cluster. However, vSphere Lifecycle Manager generates pre-validated images include a recommended firmware version for the hosts in your vSAN cluster. For more information about vSphere Lifecycle Manager recommended images, see Recommended Images.

Remediation Specifics of vSAN Clusters

Whether you manage a vSAN cluster with baselines or with a single image, remediating the hosts that are part of a vSAN cluster has its specifics.

When you remediate hosts that are part of a vSAN cluster, you must be aware of the following behavior:

- vSphere Lifecycle Manager puts only one host at a time in maintenance mode.
- vSphere Lifecycle Manager remediates hosts that are part of a vSAN cluster sequentially.
- Because vSphere Lifecycle Manager handles the remediation of the hosts sequentially, the host remediation process might take an extensive amount of time to finish.
- vSphere Lifecycle Manager remediates vSAN clusters with configured fault domains by upgrading all hosts from one fault domain first and then upgrading the hosts in the next fault domain.
- For a vSAN stretched cluster, vSphere Lifecycle Manager first remediates the hosts from the preferred site and then proceeds with remediating the hosts in the secondary site.

Host Maintenance Mode and vSAN Clusters

You can remediate a host that is in a vSAN cluster in two ways, depending on how you want to handle the virtual machines on the host:

- You can put the host in maintenance mode manually and remediate the host by using vSphere Lifecycle Manager.
- You can have the host enter maintenance mode during the vSphere Lifecycle Manager remediation process.

In the vSphere Client, when you put a host from a vSAN cluster into maintenance mode, you can choose between multiple options: Ensure accessibility, Full data evacuation, and No data evacuation. The Ensure accessibility option is the default option, and means that when you put a host in maintenance mode, vSAN ensures that all accessible virtual machines on the host remain accessible. To learn more about each of the options, see the "Place a Member of a vSAN Cluster in Maintenance Mode" topic in the *vSphere Storage* documentation.

During remediation, vSphere Lifecycle Manager, puts the hosts from the vSAN cluster in maintenance mode and handles the virtual machines on the host in the manner of the default Ensure accessibility option.

If a host is a part of a vSAN cluster, and any virtual machine on the host uses a VM storage policy with the setting for "Number of failures to tolerate=0", the host might experience unusual delays when it enters maintenance mode. The delay occurs because vSAN has to migrate the virtual machine data from one disk on the vSAN datastore cluster to another. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files on the vSAN datastore.

vSAN Health Check

vSphere Lifecycle Manager performs a remediation pre-check of vSAN clusters to ensure successful remediation. The vSAN health check is part of the remediation pre-check.

The vSAN health check gives you information about the cluster state and whether you must take extra actions to ensure successful remediation. Even if you do not take the recommended actions, you can still remediate the vSAN cluster or a host from the cluster. vSphere Lifecycle Manager successfully puts the host in maintenance mode and applies software updates on the host successfully. However, the host might fail to exit maintenance mode, and the remediation process might fail. As a result, the host from the vSAN cluster is upgraded, but you must take manual steps to take the host out of maintenance mode.

Updating Firmware in vSAN Clusters

Starting with vSphere 7.0, you can use vSphere vSphere Lifecycle Manager images to upgrade the firmware of the servers that run in your vSAN clusters.

In a vSAN cluster, the SCSI controller firmware and the physical drive firmware are handling most of the data communication. To ensure your vSAN cluster health, you must perform controller firmware updates, when necessary.

Because firmware updates affect the hardware layer in your vSphere environment, they usually are rare events. Firmware updates occur during initial ESXi host setup or during major updates of vSphere or vSAN.

In earlier vSphere releases, firmware updates are delivered as baselines in the vSAN-managed baseline group. You must use a special vendor-provided tool that vSAN uses to detect, download, and install firmware updates.

Starting with vSphere 7.0, the recommendation baseline group contains only patch updates and driver updates. It no longer contains firmware updates. As a result, you cannot use baselines to update the firmware in your vSAN clusters if the ESXi hosts are of version 7.0 or later. You can still use baselines to perform firmware updates on hosts of earlier versions, for example 6.7. But to perform firmware updates on hosts that are of version 7.0 and later and that are in a vSAN cluster, you must manage that cluster with a single image. You must also deploy an OEM-provided hardware support manager and register it as a vCenter Server extension. The hardware support manager inspects the hardware of the hosts in the cluster and lists available and compatible firmware versions, which you can add to the image for the cluster. The actual firmware update happens upon remediating the cluster against an image that contains a firmware add-on.

For more information about the requirements for using images, see System Requirements for Using vSphere Lifecycle Manager.

For more information about performing firmware updates by using images, see Firmware Updates.

Using vSphere Lifecycle Manager Images to Remediate vSAN Stretched Clusters

When you manage a vSAN stretched cluster or a two-node ROBO cluster with a single image, vSphere Lifecycle Manager can manage both the hosts in the cluster and the dedicated witness host. That is, you can check the compliance status of the witness host and remediate it against the cluster image.

What Is a Stretched Cluster?

A stretched cluster is a deployment model in which two or more hosts are part of the same logical cluster but are located in separate geographical locations. Every vSAN stretched cluster or two-node ROBO cluster has a witness host, which is a standalone host that is not a member of the respective cluster but is associated with it. The witness host of a vSAN cluster is managed by the same vCenter Server where the respective stretched or ROBO cluster resides.

vSphere Lifecycle Manager and the vSAN Witness Hosts

The vSAN witness host is a physical or virtual ESXi host that contains the witness components of virtual machine objects stored in the vSAN cluster. The witness host does not support workloads and is not a data node. A single stretched or two-node ROBO cluster can have only one witness host.

In earlier vSphere releases, you can use a single vSphere Lifecycle Manager image to manage the hosts in a vSAN stretched cluster or a two-node ROBO cluster, but the only way to manage the witness host is through vSphere Lifecycle Manager baselines. Starting with vSphere 7.0 Update 3, you can use vSphere Lifecycle Manager images to manage a vSAN stretched cluster and its witness host. The following requirements exist:

- vCenter Server must be version 7.0 Update 3 and later.
- The witness host must be ESXi version 7.0 Update 2 and later.
- The witness host must be a virtual server and not a physical server.
- The witness host must be a dedicated witness host and not a shared witness host.

You start using vSphere Lifecycle Manager images to manage the witness host by performing any of the following tasks:

- You switch from using vSphere Lifecycle Manager baselines to using vSphere Lifecycle Manager images for an existing vSAN stretched or two-node ROBO cluster.
  Note: The transition to using images is not blocked if the witness host is of ESXi version earlier than 7.0 Update 2. However, in this case, after the transition, you use a single vSphere Lifecycle Manager image for the cluster, but you must still use vSphere Lifecycle Manager baselines for the witness host. In such cases, you can use baslines to upgrade the witness host to version 7.0 Update 2, and then you can start managing the witness host with images.
- You convert an existing vSAN cluster that uses a single image into a stretched cluster with a virtual witness host.
- You upgrade to vCenter Server and the witness host to version 7.0 Update 3.

You stop using vSphere Lifecycle Manager images to manage the witness host in the following cases:

- You convert an existing vSAN stretched cluster that uses images into a regular vSAN cluster.
- You deactivate vSAN on an existing vSAN stretched cluster that you manage with a single image.
- You convert the dedicated witness host into a shared witness host.
- You replace the virtual witness host with a physical server.

Upgrading vSAN Stretched Clusters by Using a vSphere Lifecycle Manager Image

For stretched vSAN clusters, vSphere Lifecycle Manager first upgrades the witness hosts and then proceeds to remediating the hosts in the preferred site and the secondary site. If all the hosts in the preferred site are in a compliant state, then vSphere Lifecycle Manager skips the preferred site and starts remediating the hosts from the secondary site. If any host in the entire cluster is in an incompatible state, remediation stops. For more information about fault domain-aware remediation and the order in which vSphere Lifecycle Manager remediates the hosts in a vSAN cluster, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains .

During remediation, vSphere Lifecycle Manager does not apply to the witness host the full cluster image but only the base ESXi image. That is, vSphere Lifecycle Manager does not install any user components, solution components, or OEM add-ons on the witness host. The hosts in the cluster, however, are remediated against the entire image.

To remediate the witness host against the vSphere Lifecycle Manager cluster image, the following requirements exist:

- vCenter Server must be version 7.0 Update 3 and later.
- The witness host must be ESXi version 7.0 Update 2 and later.
- The witness host must be a virtual server and not a physical server.
- The witness host must be a dedicated witness host and not a shared witness host.

Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains

In vSAN clusters with configured fault domains, vSphere Lifecycle Manager remediates the hosts in an order that vSphere Lifecycle Manager calculates by factoring in the defined fault domains.

What Is a Fault Domain?

A fault domain consists of one or more vSAN hosts grouped according to their physical location in the data center. When configured, fault domains enable vSAN to tolerate failures of entire physical racks as well as failures of a single host, capacity device, network link, or a network switch dedicated to a fault domain. You can configure fault domains for non-stretched and stretched vSAN clusters. For more information about configuring fault domains, see the *Administering VMware vSAN* documentation.

Upgrading vSAN Clusters Configured with Multiple Fault Domains

vSphere Lifecycle Manager remediates vSAN clusters with configured fault domains by remediating all hosts in one fault domain at a time. To define the order of fault domains, vSphere Lifecycle Manager calculates and assigns priority to each fault domain for the vSAN cluster.

Remediation starts with the fault domain that has the highest priority. The priority of a fault domain is determined by the number of non-compliant hosts in that fault domain. The fewer non-compliant hosts in a fault domain, the higher the priority of that fault domain. However, if multiple fault domains have the same priority, vSphere Lifecycle Manager selects the first fault domain from the list of fault domains.

After vSphere Lifecycle Manager selects a fault domain, vSphere Lifecycle Manager uses DRS recommendations to select the optimal host within that domain to be remediated.

For fault domain-aware remediation of vSAN clusters, the following requirements exist:

- vCenter Server must be version 7.0 Update 1 and later
- The ESXi hosts must be version 7.0 and later

Upgrading vSAN Clusters Enabled with VMware NSX-T Data Center™ or vSphere with Tanzu

You can remediate a vSAN cluster against a vSphere Lifecycle Manager image that contains the same ESXi version as the ESXi version currently on the hosts, but the latest versions of VMware NSX-T Data Center™ and vSphere with Tanzu components. In that case, vSphere Lifecycle Manager upgrades only those components, without upgrading the ESXi version. Even in those cases, vSphere Lifecycle Manager still recognizes the configured fault domains for the vSAN cluster and performs the solution upgrade in accordance with the fault domain configuration.

For fault domain-aware remediation of vSAN clusters with enabled VMware NSX-T Data Center™ or vSphere with Tanzu, the following requirements exist:

- vCenter Server must be version 7.0 Update 2
- The ESXi hosts version 7.0 and later

About Recommendation Baseline Groups

vSAN creates system-managed baseline groups called recommendation baseline groups. You use recommendation baseline groups to upgrade the hosts in a vSAN cluster to the latest supported ESXi version, to patch the hosts with critical patches, or to update drivers on the host.

vSAN generates recommendation baseline groups automatically. If your vSphere environment does not contain any vSAN clusters, no recommendation baseline groups are generated. For each vSAN cluster in the vSphere inventory, vSphere Lifecycle Manager displays a single recommendation baseline group. You cannot edit or delete a recommendation baseline group and you cannot add it to custom baseline groups.

Recommendation baseline groups can contain any of the following sftware updates:

- An upgrade baseline that contains an ESXi upgrade image by a certified vendor with the latest tested and recommended version for the vSAN cluster.
- One or multiple patch baselines that contain recommended critical patches for the ESXi version of the hosts in the vSAN cluster.
- Recommended drivers for the ESXi hosts in the vSAN cluster.

Note: Starting with vSphere 7.0, recommendation baseline groups no longer contain firmware updates. To update the firmware on your hosts, you must convert to using a single image for the vSAN cluster.

How Does vSphere Lifecycle Manager Generate Recommendation Baselines?

A vSAN recommendation engine regularly checks the current state of the software installed on the hosts in the vSAN cluster against the vSAN Hardware Compatibility List (HCL). If update recommendations are detected, the engine downloads all new critical patches and upgrade images and generates a vSAN cluster-level baseline. All available baselines are packed together in a recommendation baseline group and made available for use by vSphere Lifecycle Manager.

Every 24 hours, vSphere Lifecycle Manager runs an automatic check for a recommendation baseline group with build recommendations coming from vSAN. If a new recommendation baseline group is detected, vSphere Lifecycle Manager automatically attaches the vSAN recommendation baseline group to the vSAN cluster.

After refreshing the vSAN recommendation baseline group, vSphere Lifecycle Manager automatically performs a compliance check operation on the vSAN clusters against the updated recommendation baseline group. Operations such as adding and removing hosts from an existing vSAN cluster also trigger refresh of the attached recommendation baseline group, followed by a compliance check.

System Requirements for Using vSAN Recommendation Baseline Groups

- vCenter Server 7.0.
  vSphere Lifecycle Manager runs as a service in vCenter Server 7.0 and later.

- vSAN cluster that contains hosts of ESXi version 6.0 Update 2 and later.
- Constant access of the vSphere Lifecycle Manager host machine to the Internet.

Configure vSphere Lifecycle Manager Remediation Settings for vSAN Clusters that You Manage with vSphere Lifecycle Manager Baselines

You can configure what type of baseline to include in the recommendation baseline group that vSphere Lifecycle Manager generates for a vSAN cluster.

- Verify that you manage the vSAN cluster with vSphere Lifecycle Manager baselines and not a single vSphere Lifecycle Manager image.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

A recommendation baseline group can contain upgrades or only host patches and updates. By default, vSphere Lifecycle Manager is set to generate recommendation baselines that contain upgrades, not only patches and updates. However, you can change the default configuration at any time. For any vSAN cluster that you manage with baselines, you can also configure vSphere Lifecycle Manager to generate no recommendation baseline group at all. In such cases, you can still manually create baselines and perform host upgrades.

1. In the vSphere Client, navigate to a vSAN cluster that you manage with baselines.
2. On the **Updates** tab, select **Hosts** > **Cluster Settings**.
3. In the **Remediation Settings for this Cluster** pane, click the **Edit** button.
   The **Edit Cluster Remediation Settings** dialog box appears.
4. Select what type of baseline to include in the recommendation baseline group that vSphere Lifecycle Manager generates for the selected vSAN cluster.
   - To include upgrade baselines into the recommendation baseline group for that cluster, select the **Include upgrades to new ESXi versions** radio button.

     The **Include upgrades to new ESXi versions** options is the default selection for any newly created vSAN cluster.
   - To include only patches and updates in the recommendation baseline group for that cluster, select the **Include patches and updates for current ESXi version** radio button.
   - To stop the generation of the recommendation baseline group for that cluster, select the **No recommendation** baseline group.
5. Click the **Done** button to save your selection and exit the dialog box.

   The option that you select becomes the default configuration for the vSAN cluster.

vSphere Lifecycle Manager and vSphere with Tanzu

You can enable vSphere with Tanzu on vSphere clusters that you manage with a single vSphere Lifecycle Manager image.

vSphere Lifecycle Manager and vSphere with Tanzu with vSphere Networking

You start using vSphere with Tanzu with vSphere networking on a cluster that uses a single vSphere Lifecycle Manager image by enabling the cluster for **Workload Management**. A cluster enabled for **Workload Management** is called a Supervisor Cluster. You enable a cluster for **Workload Management** from the **Workload Management** user interface in the vSphere Client.

Requirements

- Verify that all ESXi hosts in the Supervisor Cluster are version 7.0 Update 1 and later.

- Verify that the ESXi hosts in the Supervisor Cluster are assigned the VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes license.
- Verify that vCenter Server is version 7.0 Update 1 and later.
- **Note:** You can manage the lifecycle of a Supervisor Cluster with either vSphere Lifecycle Manager baselines or vSphere Lifecycle Manager images. However, you cannot convert a Supervisor Cluster that uses vSphere Lifecycle Manager baselines to a Supervisor Cluster that uses vSphere Lifecycle Manager images. To use vSphere Lifecycle Manager images for a Supervisor Cluster, you must first switch the cluster which is not yet enabled for **Workload Management** to using images and then enable vSphere with Tanzu on that cluster.
- Review the configuration requirements and additional information in *Working with vSphere Lifecycle Manager* chapter in the documentation.

Supported Workflows

The following workflows are supported for any Supervisor Cluster that uses vSphere Lifecycle Manager images and is configured to use the vSphere networking stack.

- You can upgrade a Supervisor Cluster to the latest version of vSphere with Tanzu. You can also upgrade the ESXi version of the hosts in the Supervisor Cluster.

  You perform the upgrade of the Supervisor Cluster from the **Workload Management** user interface in the vSphere Client.

  You upgrade the ESXi version of the hosts in the Supervisor Cluster by remediating the cluster from the vSphere Lifecycle Manager user interface in the vSphere Client.

  Note: You cannot perform a simultaneous upgrade of both vSphere with Tanzu and ESXi.
- You deactivate vSphere with Tanzu from the **Workload Management** user interface in the vSphere Client.You can deactivate vSphere with Tanzu on a cluster that uses a single vSphere Lifecycle Manager image.

  When you deactivate vSphere with Tanzu, you can use the cluster for traditional virtual machine workloads.
- You can add and remove hosts to and from a cluster that has both vSphere with Tanzu and vSphere Lifecycle Manager enabled.

  For more information about adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.

For detailed information about working with a Supervisor Cluster that uses a single image, see the *Working with vSphere Lifecycle Manager* chapter in the documentation.

Upgrading the vSphere with Tanzu Components in a vSAN Cluster

To upgrade the vSphere with Tanzu components installed on the hosts in a cluster, you must remediate the cluster against a vSphere Lifecycle Manager image that contains the latest version of those vSphere with Tanzu components.

In a vSAN cluster with configured fault domains, vSphere Lifecycle Manager recognizes the configured fault domains for the cluster and performs the solution upgrade in accordance with the fault domain configuration. If the vSAN cluster is a stretched cluster, you must upgrade the witness host separately, after vSphere Lifecycle Manager finishes remediating all fault domains. For more information about remediating vSAN stretched clusters and vSAN clusters configured with fault domains, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains . For more information about stretched clusters, see the *vSAN Planning and Deployment* documentation.

Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

vSphere Lifecycle Manager and vSphere with Tanzu with NSX-T Data Center Networking

You can start using vSphere with Tanzu with NSX-T Data Center networking on a cluster that uses a single vSphere Lifecycle Manager image by enabling the cluster for **Workload Management**. A cluster enabled with **Workload Management** is called a Supervisor Cluster. You enable the cluster for **Workload Management** from the **Workload Management** user interface in the vSphere Client. Upon enabling **Workload Management** on a Supervisor Cluster configured with the NSX networking stack, vSphere Lifecycle Manager installs the Spherelet VIB on every ESXi host in the cluster.

Requirements

- Verify that all ESXi hosts in the Supervisor Cluster are version 7.0 Update 2 or later.
- Verify that all ESXi hosts in the Supervisor Cluster are assigned the VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes license.
- Verify that vCenter Server is version 7.0 Update 2 or later.
- **Note:** You can manage the lifecycle of a Supervisor Cluster with either vSphere Lifecycle Manager baselines or vSphere Lifecycle Manager images. However, you cannot convert a Supervisor Cluster that uses vSphere Lifecycle Manager baselines to a Supervisor Cluster that uses vSphere Lifecycle Manager images. To use vSphere Lifecycle Manager images for a Supervisor Cluster, you must first switch the cluster which is not yet enabled for **Workload Management** to using images and then enable vSphere with Tanzu on that cluster.
- Review the configuration requirements and additional information in the *Working with vSphere Lifecycle Manager* chapter in the documentation.

Supported Workflows

The following workflows are supported for any Supervisor Cluster that uses vSphere Lifecycle Manager images and is configured to use the NSX-T Data Center networking stack.

- You can upgrade a Supervisor Cluster to the latest version of vSphere with Tanzu. You can also upgrade the ESXi version of the hosts in the Supervisor Cluster.

  You perform the upgrade of the Supervisor Cluster from the **Workload Management** user interface in the vSphere Client. During upgrade, vSphere Lifecycle Manager upgrades the Spherelet VIB on the hosts to make it compatible with the new version of vSphere with Tanzu or the new version of ESXi.

  You upgrade the ESXi version of the hosts in the Supervisor Cluster by remediating the cluster from the vSphere Lifecycle Manager user interface in the vSphere Client.

  Note: You cannot perform a simultaneous upgrade of both vSphere with Tanzu and ESXi.
- You deactivate vSphere with Tanzu from the **Workload Management** user interface in the vSphere Client.You can deactivate vSphere with Tanzu on a cluster that uses a single vSphere Lifecycle Manager image.

  When you deactivate vSphere with Tanzu, you can use the cluster for traditional virtual machine workloads.
- You can add and remove hosts to and from a Supervisor Cluster that uses vSphere Lifecycle Manager images.

  When you add a host to a Supervisor Cluster that you manage with a single vSphere Lifecycle Manager image, vSphere Lifecycle Manager automatically installs the Spherelet VIB on the newly added host.

  When you remove a host from a Supervisor Cluster that you manage with a single vSphere Lifecycle Manager image, vSphere Lifecycle Manager removes the Spherelet VIB from the host. vSphere Lifecycle Manager also deletes the Spherelet VIB from a host that you move to another Supervisor Cluster.

  For more information about adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.

For detailed information about working with a Supervisor Cluster that uses a single image, see the *Working with vSphere Lifecycle Manager* chapter in the documentation.

Upgrading the vSphere with Tanzu Components in a vSAN Cluster

To upgrade the vSphere with Tanzu components installed on the hosts in a cluster, you must remediate the cluster against a vSphere Lifecycle Manager image that contains the latest version of those vSphere with Tanzu components.

In a vSAN cluster with configured fault domains, vSphere Lifecycle Manager recognizes the configured fault domains for the cluster and performs the solution upgrade in accordance with the fault domain configuration. If the vSAN cluster is a stretched cluster, you must upgrade the witness host separately, after vSphere Lifecycle Manager finishes remediating all fault domains. For more information about remediating vSAN stretched clusters and vSAN clusters configured with fault domains, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains . For more information about stretched clusters, see the *vSAN Planning and Deployment* documentation.

Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

vSphere Lifecycle Manager and VMware NSX-T Data Center™

You can use vSphere Lifecycle Manager baselines for upgrade operations in environments with VMware NSX-T Data Center™ 3.0. Starting with vSphere 7.0 Update 1 and VMware NSX-T Data Center™ 3.1, you can also use vSphere Lifecycle Manager images to manage clusters that have VMware NSX-T Data Center™ enabled.

Using vSphere Lifecycle Manager Baselines to Upgrade ESXi Hosts in an Environment With VMware NSX-T Data Center™ 3.0

You can use vSphere Lifecycle Manager to upgrade the ESXi hosts in an environment where you have VMware NSX-T Data Center™ enabled.

Requirements

- Verify that the ESXi hosts to upgrade are version 6.5 or later.
- vCenter Server version 6.7 or earlier
- VMware NSX-T Data Center™ 3.0
- Verify that the vmknics on the ESXi host are properly configured and the DHCP server works properly.

Workflow

1. Upgrade vCenter Server to version 7.0.
   For more information about upgrading vCenter Server, see the *vSphere Upgrade* documentation.
2. Import an ESXi 7.0 ISO image to the vSphere Lifecycle Manager depot.
   For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.
3. Download the VMware NSX-T Data Center™ 3.0.0 NSX Kernel Module for VMware ESXi 7.0 from http://my.vmware.com.
4. Import the kernel module to the vSphere Lifecycle Manager depot.
   For more information, see Import Updates to the vSphere Lifecycle Manager Depot.
5. Create an upgrade baseline with the imported ESXi 7.0 ISO image.
   For more information, see Create a Host Upgrade Baseline.
6. Create an extension baseline with the uploaded NSX kernel module.
   For more information, see Create a Host Extension Baseline.
7. Create a baseline group that contains the newly created upgrade and extension baselines.
   For more information, see Create a Host Baseline Group.

8. Attach the baseline group to a cluster.
   For more information, see Attach Baselines and Baseline Groups to Objects.
9. Remediate the cluster against the attached baseline group.
   For more information, see Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines.

Using vSphere Lifecycle Manager Images in an Environment With VMware NSX-T Data Center™ 3.1

You can use VMware NSX-T Data Center™ on a cluster that you manage with a single vSphere Lifecycle Manager image. As a result, you can use NSX Manager to install, upgrade, or remove NSX components on the ESXi hosts in a cluster that you manage with a single image.

Requirements

- Verify that all ESXi hosts in the cluster are version 7.0 Update 1 or later.
- Verify that vCenter Server is version 7.0 Update 1 or later.
- Verify that VMware NSX-T Data Center™ is version 3.1 or later.
- Verify that a vSphere Distributed Switch (VDS) is configured to manage the VMware NSX-T Data Center™ traffic.

Supported Workflows

The following workflows are supported for clusters that are enabled for both vSphere Lifecycle Manager images and VMware NSX-T Data Center™.

- You can enable VMware NSX-T Data Center™ on a cluster that you manage with a single vSphere Lifecycle Manager image.
  You perform the operation by configuring a transport node profile (TNP) for the cluster in the NSX Manager. In the NSX Manager, you can either manually add a TNP to the cluster, or automatically generate one in the **Getting Started** wizard. You can continue leveraging individual transport node configurations, but you must always use a TNP for the clusters that you manage with a single vSphere Lifecycle Manager image. You cannot enable VMware NSX-T Data Center™ on a cluster that uses a single vSphere Lifecycle Manager image if you choose to only use individual transport node configurations for the hosts in the cluster.
- You can add hosts to a cluster that you manage with a single vSphere Lifecycle Manager image and that is enabled with VMware NSX-T Data Center™. You can also remove hosts from such a cluster.
  You perform the add and remove host operations in the vSphere Client. When you add a host to the cluster, vSphere Lifecycle Manager automatically installs the VMware NSX-T Data Center™ component to the newly added host. To add a host to a cluster that you manage with a single vSphere Lifecycle Manager image, the host must be added to the VDS associated with the TNP. Otherwise, the host cannot fully work with VMware NSX-T Data Center™.
  When you move a host from one cluster that uses a single vSphere Lifecycle Manager image to another, vSphere Lifecycle Manager applies the target cluster's image together with the target VMware NSX-T Data Center™ component to the newly added host. If a host is deleted from the vCenter Server inventory, the VMware NSX-T Data Center™ component is uninstalled from the host.
  For more information about adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.
- You can upgrade VMware NSX-T Data Center™ 3.1 to a later version in a cluster that you manage with a single vSphere Lifecycle Manager image.
  You perform the operation from the NSX Manager.
- You can upgrade both VMware NSX-T Data Center™ and ESXi in a single vSphere Lifecycle Manager remediation task. The workflow is supported only if you upgrade from VMware NSX-T Data Center™ version 3.1.
  In the NSX Manager, you stage the VMware NSX-T Data Center™ upgrade as part of the image that the cluster uses. From the vSphere Lifecycle Manager user interface in the vSphere Client, you can further edit the image and you

initiate remediation of the cluster. During remediation, vSphere Lifecycle Manager applies both the VMware NSX-T Data Center™ and ESXi upgrades to the hosts in the cluster. For more information, see the *NSX-T Data Center Upgrade Guide* documentation.

- You can switch from using vSphere Lifecycle Manager to using a vSphere Lifecycle Manager image for a cluster that is enabled with VMware NSX-T Data Center™.
- You can uninstall VMware NSX-T Data Center™ from a host or a cluster that you manage with a single vSphere Lifecycle Manager image.
- You can check the compliance, generate a remediation pre-check report, and remediate a cluster that you manage with a single vSphere Lifecycle Manager image and that is enabled with VMware NSX-T Data Center™.

  You perform the check compliance, generate a remediation pre-check, and remediation operations in the vSphere Client. Whenever you change the VMware NSX-T Data Center™ configuration in the NSX Manager, the compliance state of the cluster that you see on the **Updates** tab for the cluster in the vSphere Client changes to non-compliant. You can remediate non-compliant hosts and clusters in the vSphere Client or you can solve the issues that cause non-compliance in the NSX Manager.
- You can back up and restore VMware NSX-T Data Center™.
- You can export the vSphere Lifecycle Manager image of a cluster that is enabled with VMware NSX-T Data Center™ and import this image to another cluster that has both vSphere Lifecycle Manager images and VMware NSX-T Data Center™ enabled.

For detailed information about all workflows that you perform in the NSX Manager, see the *NSX-T Data Center Administration* documentation.

Upgrading the VMware NSX-T Data Center™ Components in a vSAN Cluster

To upgrade the VMware NSX-T Data Center™ components installed on the hosts in a cluster, you must remediate the cluster against a vSphere Lifecycle Manager image that contains the latest version of those VMware NSX-T Data Center™ components.

In a vSAN cluster with configured fault domains, vSphere Lifecycle Manager recognizes the configured fault domains for the cluster and performs the solution upgrade in accordance with the fault domain configuration. If the vSAN cluster is a stretched cluster, you must upgrade the witness host separately, after vSphere Lifecycle Manager finishes remediating all fault domains. For more information about remediating vSAN stretched clusters and vSAN clusters configured with fault domains, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains . For more information about stretched clusters, see the *vSAN Planning and Deployment* documentation.

Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

Backup and Restore Scenarios When Using vSphere Lifecycle Manager

Restoring a vCenter Server instance from a backup might impact the clusters in your environment in a seemingly unexpected way. Whether you use images or baselines to manage your clusters, vSphere Lifecycle Manager behaves in a specific manner during backup and restore operations.

When you back up a vCenter Server instance, you create a backup copy of all clusters in that vCenter Server instance.

Restoring vCenter Server After Switching from Baselines to Images for Cluster Lifecycle Management

Cluster A is a cluster that you manage by using baselines. You back up the vCenter Server instance where the cluster is. After the backup, you switch from using baselines to using images to manage cluster A and you remediate the cluster to apply the image to the hosts in the cluster. You now manage the lifecycle of cluster A by using a single cluster image.

If for some reason you must restore the vCenter Server instance from the backup copy you created, the restored vCenter Server instance contains cluster A. Because cluster A was managed through baselines at the time when you backed up the vCenter Server system, the restored vCenter Server instance contains cluster A, but you must again use baselines to manage it.

Restoring vCenter Server After Remediating a Cluster Managed by an Image

After remediation, cluster A uses image X with components Y to manage all hosts in the cluster collectively. At a point in time T, you back up the vCenter Server system. Later, you remediate the cluster against a new image X+1 with new components Y+1. Now all hosts in the cluster use image X+1 with components Y+1.

If for some reason you must restore the vCenter Server system from the backup copy that you created at time T, the restored vCenter Server instance contains cluster A, but the compliance check lists the hosts in the cluster as incompatible with the image that cluster A uses. The reason for the incompatibility is that after the restore operation, cluster A reverts back to using image X with components Y, while the hosts in the cluster still run image X+1 with components Y+1. Because you cannot downgrade ESXi, to make the hosts compliant with the cluster image, you must upgrade the cluster to image X+1 with components Y+1.

Upgrading Virtual Machines with vSphere Lifecycle Manager

You can use vSphere Lifecycle Manager to upgrade virtual machine hardware and the VMware Tools version of a virtual machine.

Whether you perform an upgrade of the virtual machine hardware version or the VMware Tools version, the upgrade is a multi-stage process.

1. You check the status of individual virtual machines or a container object.
   vSphere Lifecycle Manager checks the status of a virtual machine against the latest virtual machine hardware version supported by the host on which the virtual machine runs. Similarly, vSphere Lifecycle Manager checks the status of the virtual machine against the latest VMware Tools version supported by the host on which the virtual machine runs.
   For more information about checking virtual machine status, see Checking the Status of Virtual Machines.
2. You review the status of the scanned virtual machines.
3. You upgrade the virtual machine to match the host where it resides.
   With vSphere Lifecycle Manager, you can upgrade the virtual machine hardware version and the VMware Tools version that a virtual machine has. You can use vSphere Lifecycle Manager to upgrade the virtual machine hardware version to the latest hardware version, vmx-19, and to the latest VMware Tools version on the hosts.
   For more information about upgrading virtual machines, see Upgrading Virtual Machines.

Configure Virtual Machine Rollback Settings

By default, vSphere Lifecycle Manager takes snapshots of virtual machines before upgrading them. If the upgrade fails, you can use the snapshot to return a virtual machine to its state before the upgrade.

Required privileges: **VMware vSphere Lifecycle Manager** > **Configure**

You can configure vSphere Lifecycle Manager to keep snapshots for an indefinite or fixed period of time. Use the following guidelines when managing snapshots.

- Keeping snapshots indefinitely might consume a large amount of disk space and degrade virtual machine performance.

- Keeping no snapshots saves space, ensures best virtual machine performance, and might reduce the remediation time. However, keeping no snapshots limits the availability of a rollback.
- Keeping snapshots for a fixed period of time uses less disk space and offers a backup for a short time.

vSphere Lifecycle Manager does not take snapshots of fault tolerant virtual machines and virtual machines of virtual machine hardware version 3. If you decide to take snapshots of such virtual machines, the upgrade might fail.

If you configure vSphere Lifecycle Manager to automatically upgrade VMware Tools on power cycle for selected virtual machines, vSphere Lifecycle Manager does not take snapshots of the virtual machines before upgrading them and you cannot roll back.

1. Navigate to the vSphere Lifecycle Manager home view.
   a) In the vSphere Client, select **Menu** > **Lifecycle Manager**.
   b) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Host Remediation** > **VMs**.
3. Click the **Edit** button.

   The **Edit Default Settings for VM Rollback** dialog box opens.
4. Select the **Take snapshot of VMs** check box.
5. Select the time period for keeping the snapshots.
   - Do not delete snapshots
   - Keep snapshots for a configurable, fixed period of time
6. Click **Save** to save your changes and close the **Edit Default Settings for VM Rollback** dialog box.

These settings become the default rollback option settings for virtual machines. You can specify different settings when you configure individual remediation tasks.

Checking the Status of Virtual Machines

You use vSphere Lifecycle Manager to check the status of virtual machines before you upgrade them. The status check shows if the virtual machine is up-to-date or can be upgraded.

With vSphere Lifecycle Manager, you can check the status of a single virtual machine or a group of virtual machines in a parent container object.

Supported groups of virtual machines or ESXi hosts include virtual infrastructure container objects such as folders, vApps, clusters, and data centers.

vSphere Lifecycle Manager checks the status of virtual machines in two aspects.

- You can use vSphere Lifecycle Manager to check the status of the virtual machines in respect with the VMware Tools version that they have installed.

  The status check is performed against the latest VMware Tools version that the parent host supports.
- vSphere Lifecycle Manager checks the status of the virtual machines in respect with their VM hardware compatibility.

  vSphere Lifecycle Manager compares the hardware compatibility of the virtual machines with the default VM hardware compatibility configured for the host.

Check the Status of an Individual Virtual Machine

You check the status of virtual machines to see whether the VMware Tools version they have is up to date and whether their hardware compatibility matches the default VM hardware compatibility for the host.

1. In the vSphere Client, navigate to a virtual machine.
2. On the **Updates** tab, click **Check Status**.

   The **Scan entity** task appears in the **Recent Tasks** pane. After the task finishes, status information appears in the **VMware Tools** and **VM Hardware Compatibility** panels.

The virtual machines are scanned for VMware Tools and VM hardware compliance.

Check the Status of the Virtual Machines in a Container Object

You check the status of virtual machines to see whether the VMware Tools version they have is up-to-date and whether their hardware compatibility matches the default VM hardware compatibility for the host where they reside.

When you perform a status check for a container object, vSphere Lifecycle Manager checks the VMware Tools and VM Hardware Compatibility statuses for all child virtual machines. The larger the virtual infrastructure and the higher up in the object hierarchy you initiate the status check, the longer the task takes.

1. In the vSphere Client, navigate to a virtual machine container object, such as a virtual machine folder, host, cluster, and so on.
2. Click the **Updates** tab.
3. Select your task.

Option	Action
Check the VMware Tools status of the virtual machines in the container object.	1. Select **Hosts** > **VMware Tools** > . 2. Click **Check Status**. The information about the VMware Tools status appears in the **Tools Status** column in the table that lists all virtual machines in the selected container object. If the container object is a data center or a vCenter Server instance, you must first specify the cluster that you want to see results for.
Check the VM Hardware compatibility status of the virtual machines in the container object.	1. Select **Hosts** > **VM Hardware**. 2. Click **Check Status**. The information about the VM Hardware Compatibility status appears in the **Status** column in the table that lists all virtual machines in the selected container object. For each virtual machine in the object, you can also see the VM hardware compatibility and the host compatibility. If the container object is a data center or a vCenter Server instance, you must first specify the cluster that you want to see results for.

The VMware Tools Status

Check the VMware Tools status for information whether the current version of VMware Tools is installed, supported, or whether upgrades are available.

Table 127: VMware Tools Status

VMware Tools Status	Description
Up to Date	VMware Tools is installed, supported, and the version is compliant.
	VMware Tools is installed, supported, and the version is newer than the version available on the ESXi host.
Upgrade Available	VMware Tools is installed, but the version is old.
	VMware Tools is installed and supported, but a newer version is available on the ESXi host.
Version Unsupported	VMware Tools is installed, but the version is old.
	VMware Tools is installed, but the version has a known issue and must be immediately upgraded.
	VMware Tools is installed, but the version is too new to work correctly with this virtual machine.
Not Installed	VMware Tools is not installed on this virtual machine.
Guest Managed	vSphere does not manage VMware Tools.
Unknown	The status of the virtual machine is not checked.

Upgrading Virtual Machines

With vSphere Lifecycle Manager, you can upgrade the VMware Tools version and the hardware version of a virtual machine. You can also upgrade multiple virtual machines simultaneously if the virtual machines are in a container object, such as a folder or vApp. You can also upgrade simultaneously all virtual machines that run on a host, in a cluster, or in a data center.

vSphere Lifecycle Manager supports upgrading powered on, suspended, and powered off virtual machines.

During the upgrade of VMware Tools, the virtual machines must be powered on. If a virtual machine is in the powered off or suspended state before remediation, vSphere Lifecycle Manager powers it on. After the upgrade completes, vSphere Lifecycle Manager restarts the machine and restores the original power state of the virtual machine.

During the virtual hardware upgrade, the virtual machines must be powered off. If a virtual machine is powered on, vSphere Lifecycle Manager powers the machine off, upgrades the virtual hardware, and then powers the virtual machine on.

You can also upgrade VMware Tools and the hardware version of a virtual machine template. A template is a copy of a virtual machine that you can use to create and provision new virtual machines.

You can set up automatic upgrades of VMware Tools on power cycle. For more information, see Automatically Upgrade VMware Tools on Reboot.

You can configure vSphere Lifecycle Manager to take snapshots of virtual machines and to keep the snapshots indefinitely or for a specific period of time. By using snapshots, you can roll back a virtual machine to its previous state if upgrading the virtual machine with vSphere Lifecycle Manager fails. After the upgrade finishes, you can delete the snapshots if you do not need them. For more information about configuring virtual machine rollback settings, see Configure Virtual Machine Rollback Settings.

You can upgrade virtual machines immediately or schedule an upgrade operation to run at a convenient time.

If a host is connected to vCenter Server by using an IPv6 address, you cannot scan and remediate virtual machines that run on the host.

Upgrade the VM Hardware Compatibility of Virtual Machines

You can upgrade the hardware of virtual machines to the latest hardware version that the host supports. You can upgrade immediately or schedule an upgrade at a time that is convenient for you.

With vSphere Lifecycle Manager, you can upgrade the hardware compatibility version of a single virtual machine or multiple virtual machines simultaneously. Supported container objects for virtual machines in the vSphere inventory are folders, vApps, data centers.

1. In the vSphere Client, navigate to a single virtual machine or a container object.

   You can also initiate upgrade at the level of any inventory object where virtual machines run. For example, you can start the upgrade operation at a host or cluster level.

2. Open the **Upgrade VM Hardware to Match Host** dialog box.

Inventory Object	Steps
Virtual Machine	1. Click the **Updates** tab. 2. In the **VM Hardware Compatibility** panel, click **Upgrade to Match Host**.
Container Object, Host, Cluster, Data Center, or vCenter Server Instance	1. Click the **Updates** tab. 2. Select **Hosts** > **VM Hardware**. 3. If the selected inventory object is a data center or a vCenter Server instance, select a cluster from the list. A list of all virtual machines in the cluster appears in the bottom pane. 4. Select the virtual machines to upgrade. 5. Click **Upgrade to Match Host**.

   A list of the virtual machines selected for upgrading is visible in the **Upgrade VM Hardware to Match Host** dialog box.

3. Optional: To change the selection of the virtual machines to upgrade, select or deselect virtual machines from the list.
4. Optional: To schedule the upgrade for a specific date and time, expand **Scheduling Options** and configure the scheduled task.
   a) Enter a name and, optionally, a description for the scheduled upgrade task.
   b) Use the **Powered On VMs**, **Powered Off VMs**, and **Suspended VMs** drop-down menus to configure the upgrade to run immediately or at a specific date and time.
5. Optional: To configure the use of snapshots, expand **Rollback Options** and change the default settings.
   a) To allow or disallow taking of snapshots of virtual machines before upgrading them, select or deselect the **Take snapshot of VMs** check box.

      The option to take snapshots is selected by default.
   b) Select a period for keeping the snapshots.
      - Keep the snapshots indefinitely.
      - Keep the snapshots for a fixed period.
   c) Enter a snapshot name and, optionally, a description for the snapshot.
   d) Include the virtual machine memory in the snapshot by selecting the respective check box.
6. Review your selections and click the **Upgrade to Match Host** button.

The hardware versions of the selected virtual machines are upgraded and the virtual machine status changes to Up to Date.

Upgrade the VMware Tools Version of Virtual Machines

You can upgrade the VMware Tools version of virtual machines to the latest version that the host supports. You can upgrade immediately or schedule an upgrade at a time that is convenient for you.

With vSphere Lifecycle Manager, you can upgrade the VMware Tools version of a single virtual machine or multiple virtual machines simultaneously. Supported container objects for virtual machines in the vSphere inventory are folders, vApps, data centers.

1. In the vSphere Client, navigate to a single virtual machine or a container object.

   You can initiate the upgrade at the level of any inventory object where virtual machines run. For example, you can start the upgrade operation at a host or cluster level.

2. Open the **Upgrade VMware Tools to Match Host** dialog box.

Inventory Object	Steps
Virtual Machine	1. Click the **Updates** tab. 2. In the **VMware Tools** panel, click **Upgrade to Match Host**.
Container Object, Host, Cluster, Data Center, or Instance	1. Click the **Updates** tab. 2. Select **Hosts** > **VMware Tools**. 3. If the selected inventory object is a data center or a instance, select a cluster from the list. A list of all virtual machines in the cluster appears in the bottom pane. 4. In the **VMs in Cluster** pane, select the virtual machines to upgrade. 5. Click **Upgrade to Match Host**.

   A list of the virtual machines selected for upgrading is visible in the **Upgrade VMware Tools to Match Host** dialog box.

3. Optional: To change the selection of the virtual machines to upgrade, select or deselect virtual machines from the list.
4. Optional: To schedule the upgrade for a specific date and time, expand **Scheduling Options** and configure the scheduled task.
   a) Enter a name and, optionally, a description for the scheduled upgrade task.
   b) Use the **Powered On VMs**, **Powered Off VMs**, and **Suspended VMs** drop-down menus to configure the upgrade to run immediately or at a specific date and time.
5. Optional: To configure the use of snapshots, expand **Rollback Options** and change the default settings.
   a) To allow or disallow taking of snapshots of virtual machines before upgrading them, select or deselect the **Take snapshot of VMs** check box.

      The option to take snapshots is selected by default.
   b) Select a period for keeping the snapshots.
      - Keep the snapshots indefinitely.
      - Keep the snapshots for a fixed period.
   c) Enter a snapshot name and, optionally, a description for the snapshot.
   d) Include the virtual machine memory in the snapshot by selecting the respective check box.
6. Review your selections and click the **Upgrade to Match Host** button.

The VMware Tools version that runs on the selected virtual machines is upgraded and the VMware Tools status changes to Up to Date.

Automatically Upgrade VMware Tools on Reboot

You can automate the process of upgrading VMware Tools for the virtual machines in your inventory.

Verify that you have the **VcIntegrity.Updates.com.vmware.vcIntegrity.Remediate** privilege.

You can set up vSphere Lifecycle Manager to check the VMware Tools version of a virtual machine when the virtual machine is rebooted. If necessary, vSphere Lifecycle Manager upgrades VMware Tools to the latest version supported by the host on which the virtual machine runs.

Note:

When you perform a VMware Tools upgrade on power cycle, vSphere Lifecycle Manager does not take a snapshot of the virtual machine and you cannot roll back to the previous version of the virtual machine.

1. In the vSphere Client, navigate to a single virtual machine or an inventory object that contains virtual machines.
2. Configure vSphere Lifecycle Manager to automatically upgrade VMware Tools on reboot.

Inventory Object	Steps
Virtual machine	1. Click the **Updates** tab. 2. In the **VMware Tools** panel, click **Turn On**.
Container Object, Host, cluster, data center, or vCenter Server instance	1. Click the **Updates** tab. 2. Select **Hosts** > **VMware Tools**. 3. If the selected inventory object is a data center or a vCenter Server instance, select a cluster from the list. A list of all virtual machines in the cluster appears in the bottom pane. 4. In the **VMs in cluster** pane, select the virtual machines for which you want to enable the automatic upgrade of VMware Tools. 5. Click **Set Auto Update** and select **On**. The new status is visible in the **Auto Update** column.

The next time you power on or restart a virtual machine, vSphere Lifecycle Manager checks the version of VMware Tools installed on the virtual machines and performs an upgrade, if necessary.

Installing, Setting Up, and Using Update Manager Download Service

VMware vSphere Update Manager Download Service (UMDS) is an optional module of vSphere Lifecycle Manager. UMDS downloads patch metadata, patch binaries, and notifications that might not otherwise be available to vSphere Lifecycle Manager.

For security reasons and deployment restrictions, vSphere, including vSphere Lifecycle Manager, might be installed in a secured network that is disconnected from other local networks and the Internet. vSphere Lifecycle Manager requires access to patch information to function properly. If you are using such an environment, you can install UMDS on a computer that has Internet access to download upgrades, patch binaries, and patch metadata, and then export the downloads to a portable media drive so that they become accessible to the vSphere Lifecycle Manager.

Note:

The URLs of the official VMware online depot are now unique for each customer. To update the download sources URLs, see the following KB articles: https://knowledge.broadcom.com/external/article/390121 and https://knowledge.broadcom.com/external/article/390123.

If the server on which vCenter Server is installed has no Internet access, but is connected to a server that has Internet access, you can automate the export process and transfer files from UMDS to the vSphere Lifecycle Manager depot by using a Web server on the machine on which UMDS is installed.

UMDS 7.0 supports patch recalls and notifications. A patch is recalled if the released patch has problems or potential issues. After you download patch data and notifications with UMDS, and export the downloads so that they become available to vSphere Lifecycle Manager, vSphere Lifecycle Manager deletes the recalled patches.

Starting with vSphere 7.0, the UMDS is available for installation only on Linux-based operating systems. Installing UMDS on a Windows machine is no longer supported. Administrator access is not a requirement for downloading patches with UMDS that runs on Linux. The machine on which you install UMDS must have Internet access.

vSphere Lifecycle Manager supports using UMDS for both images and baselines. That is, UMDS downloads updates that are packaged and distributed as bulletins, but it also works with components, which are the main software update package in vSphere 7.0

Compatibility Between UMDS and vSphere Lifecycle Manager

UMDS must be of the same version as vSphere Lifecycle Manager.

For example, vSphere Lifecycle Manager7.0 is compatible and can work only with UMDS 7.0. If you are using vSphere Lifecycle Manager of an Update release version, UMDS must be of the same Update release version.

Installing UMDS

In vSphere 7.0 release, the UMDS 7.0 is bundled with the vCenter Server appliance 7.0. You can use the UMDS bundle from the vCenter Server appliance to install UMDS 7.0 on a separate Linux-based system.

UMDS is a 64-bit application and requires a 64-bit Linux-based system.

Note: You cannot upgrade UMDS that runs on a Linux-based operating system. You can uninstall the current version of UMDS, perform a fresh installation of UMDS according to all system requirements, and use the existing patch store from the UMDS that you uninstalled.

Supported Linux-Based Operating Systems for Installing UMDS

The Update Manager Download Service (UMDS) can run on a limited number of Linux-based operating systems.

- Ubuntu 14.0.4
- Ubuntu 18.04
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 8.1

  Note: When you use Red Hat Enterprise Linux 8.1, you must install the libnsl package version 2.28 or later on the system where UMDS is deployed. If the package is not present on the system, UMDS operations might fail with the following error:

  ```
  Error while loading shared libraries: libnsl.so.1: cannot open shared object file: No
   such file or directory.
  ```
- Red Hat Enterprise Linux 8.3
- Red Hat Enterprise Linux 8.5
- Red Hat Enterprise Linux 8.6
- Red Hat Enterprise Linux 9.0

Install UMDS on a Linux OS

If the vCenter Server appliance 7.0 where vSphere Lifecycle Manager runs does not have access to the Internet, you can install UMDS on a Linux-based operating system to download update binaries and metadata.

- Verify you have administrative privileges on the Linux machine where you install the UMDS.
- Mount the ISO file of the vCenter Server appliance 7.0 to the Linux machine.

1. In the Linux machine, open the Command Shell.
2. From the vCenter Server ISO that you mounted to the Linux machine, copy the `VMware-UMDS-7.0.0-build_number.tar.gz` file to the Linux machine.
3. Unarchive the `VMware-UMDS-7.0.0-build_number.tar.gz` file by running `tar -xvzf VMware-UMDS-7.0.0-build_number.tar.gz` and navigate to the newly extracted directory `/vmware-umds-distrib`.
   For example, if you unarchived the `VMware-UMDS-7.0.0-build_number.tar.gz` file, to a directory you created with the name *umds*, your navigation path is `/umds/vmware-umds-distrib`.
4. Run the file UMDS installation script.
   The script has the following filename: `vmware-install.pl`.
5. Read and accept the EULA.
6. Select a directory where to install the UMDS.
   The default UMDS installation location is `usr/local/vmware-umds`.
7. Enter the UMDS proxy settings.
   You can also change proxy configuration after you install UMDS by using the following command:

   ```
   vmware-umds -S --proxy <proxyAddress:port>
   ```

8. Select a directory where to store the patches.

   Important: The patch store directory must be different from the UMDS installation directory. The default patch store location is `/var/lib/vmware-umds`.

UMDS is installed.

Uninstall UMDS from a Linux OS

To use the latest UMDS version on your Linux-based system, you must first uninstall the current version of UMDS. No direct upgrade path is available to a later version of UMDS.

- Verify you have administrative privileges on the Linux machine where UMDS runs.

1. In the Linux machine, open the Command Shell.
2. Navigate to the UMDS installation directory, and locate the file `vmware-uninstall-umds.pl`.
   The default UMDS installation location is `usr/local/vmware-umds`.
3. Run the `./vmware-uninstall-umds.pl` command.
4. To confirm that you want to uninstall UMDS from the system, enter **Yes**.
   The UMDS uninstallation procedure starts.
5. Optional: Remove PostgreSQL Database from you Linux machine.
   For information about uninstalling PostgreSQL Database, go to the official PostgreSQL documentation.

UMDS is uninstalled from the Linux system.

You can upgrade your Linux OS, and install a later compatible version of UMDS.

Setting Up and Using UMDS

You can set up UMDS to download patches for ESXi hosts. You can also set up UMDS to download ESXi 6.5, ESXi6.7, and ESXi7.0 patch binaries, patch metadata, and notifications from third-party portals.

Administrator access is not a requirement for downloading patches if UMDS runs on Linux.

After you download the upgrades, patch binaries, patch metadata, you can export the data to a Web server or a portable media drive and set up vSphere Lifecycle Manager to use a folder on the Web server or the media drive (mounted as a local disk) as a shared repository.

You can also set up UMDS to download ESXi 6.5, ESXi6.7, and ESXi7.0 patches from third-party portals.

To use UMDS, the machine on which you install it must have Internet access. After you download the data you want, you can copy it to a local Web server or a portable storage device, such as a CD or USB flash drive.

The best practice is to use a job scheduler, for example cron job, to create a job that periodically triggers UMDS to download the upgrades, patches, and notifications.

Set Up the Data to Download with UMDS

By default, UMDS downloads patch binaries, patch metadata, and notifications for hosts. You can specify which patch binaries and patch metadata to download with UMDS.

1. Log in to the machine where UMDS is installed, and open a **Command Prompt** window.
2. Navigate to the directory where UMDS is installed.
   The default location in 64-bit Linux is `/usr/local/vmware-umds`.
3. Specify the updates to download.
   - To set up a download of all ESXi host updates, run the following command:
     `vmware-umds -S --enable-host`
   - To deactivate the download of host updates, run the following command:
     `vmware-umds -S --disable-host`

Download the selected data.

Change the UMDS Patch Repository Location

UMDS downloads upgrades, patch binaries, patch metadata, and notifications to a folder that you can specify during the UMDS installation.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds` .

You can change the folder in which UMDS downloads data after you install UMDS.

If you have already downloaded host updates, copy all the files and folders from the old location to the new patch store location. The folder in which UMDS downloads patch binaries and patch metadata must be located on the machine on which UMDS is installed.

1. Log in as an administrator to the machine where UMDS is installed, and open a **Command Prompt** window.
2. Navigate to the directory where UMDS is installed.
   The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3. Change the patch repository directory by running the command:
   `vmware-umds -S --patch-store your_new_patchstore_folder`

   In this example, *your_new_patchstore_folder* is the path to the new folder in which you want to download the patch binaries and patch metadata.

You successfully changed the directory in which UMDS stores patch data.

Download data using UMDS.

Configure URL Addresses for Hosts

You can configure UMDS to connect to the websites of third-party vendors to download ESXi 6.5, ESXi6.7, and ESXi7.0 host patches and notifications.

1. Log in to the machine where UMDS runs, and open a **Command Prompt** window.
2. Navigate to the directory where UMDS is installed.
   The default location in 64-bit Linux is `/usr/local/vmware-umds`.
3. Configure UMDS to download data from the new URL address.
   - To add a new URL address for downloading patches and notifications for ESXi 6.5, ESXi6.7, or ESXi7.0 hosts, run the following command:
     `vmware-umds -S --add-url https://host_URL/index.xml --url-type HOST`
4. Optional: Remove a URL address, so that UMDS does not download data from it anymore.
   Downloaded data is retained and can be exported. Use the following command:
   `vmware-umds -S --remove-url https://URL_to_remove/index.xml`

You configured UMDS to download host patches and notifications from specific URL addresses.

Download the patches and notifications by using UMDS.

Download the Specified Data Using UMDS

After you set up UMDS, you can download upgrades, patches and notifications to the machine on which UMDS is installed.

Administrator level access is not a requirement for downloading data with UMDS that runs on Linux.

Note:

The URLs of the official VMware online depot are now unique for each customer. To update the download sources URLs, see the following KB articles: https://knowledge.broadcom.com/external/article/390121 and https://knowledge.broadcom.com/external/article/390123.

1. Log in to the machine where UMDS is installed, and open a **Command Prompt** window.
2. Navigate to the directory where UMDS is installed.
   The default location in 64-bit Linux is `/usr/local/vmware-umds`.
3. Download the selected updates.

```
vmware-umds -D
```

This command downloads all the upgrades, patches and notifications from the configured sources for the first time. Subsequently, it downloads all new patches and notifications released after the previous UMDS download.

4. Optional: If you have already downloaded upgrades, patches, and notifications and want to download them again, you can include the start and end times to restrict the data to download.

   The command to re-download patches and notifications deletes the existing data from the patch store (if present) and re-downloads it.

   To re-download the upgrades, patches and notifications that were downloaded in November 2010, for example, run the following command:

   ```
   vmware-umds -R --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
   ```

   The data previously downloaded for the specified period is deleted and downloaded again.

Export the downloaded upgrades, patches, and notifications.

Export the Downloaded Data

You can export downloaded upgrades, patches, and notifications to a specific location that serves as a shared repository for vSphere Lifecycle Manager. You can configure vSphere Lifecycle Manager to use the shared repository as a patch download source. The shared repository can also be hosted on a Web server.

If you installed UMDS with an existing download directory, verify that you perform at least one download by using UMDS 7.0 before you export updates.

Administrator level access is not a requirement for exporting the downloaded data with UMDS that runs on Linux.

1. Log in to the machine where UMDS is installed and open a **Command Prompt** window.
2. Navigate to the directory where UMDS is installed.

   The default location in 64-bit Linux is `/usr/local/vmware-umds`.
3. Specify the export parameters and export the data.

   ```
   vmware-umds -E --export-store repository_path
   ```

   In the command, you must specify the full path of the export directory.

   If you are working in a deployment in which the vCenter Server is installed on a machine connected to the machine on which UMDS is installed, *`repository_path`* can be the path to the folder on the Web server that serves as a shared repository.

   If the vCenter Server is installed on a machine in an isolated and secure environment, *`repository_path`* can be the path to a portable media drive. Export the downloads to the portable media drive to physically transfer the patches to the machine on which vCenter Server is installed and vSphere Lifecycle Manager runs.

   The data you downloaded by using UMDS is exported to the path you specify. Make sure that all files are exported. You can periodically export from UMDS and populate the shared repository so that vSphere Lifecycle Manager can use the new patch binaries and patch metadata.
4. Optional: You can export the ESXi patches that you downloaded during a specified time window.
   For example, to export the patches downloaded in November 2010, run the following command:

   ```
   vmware-umds -E --export-store repository-path --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
   ```

Configure vSphere Lifecycle Manager to use a shared repository as a patch download source. For more information, see Configure vSphere Lifecycle Manager to Use a Shared Repository as a Download Source.

vCenter Server Configuration

vCenter Server Appliance Configuration provides information about configuring the VMware vCenter®Server Appliance™.

Intended Audience

This information is intended for anyone who wants to configure VMware vCenter Server® . The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

vSphere Web Client and vCenter Server Management Interface

Instructions in this guide reflect thevSphere Client, an HTML5-based GUI, and thevCenter Server Management Interface. Some additional functions can be performed using thevCenter Server appliance shell and the Direct Console User Interface.

About vCenter Server Configuration

vCenter Server Configuration provides information about configuring VMware vCenter®Server™.

Intended Audience

This information is intended for anyone who wants to configure VMware vCenter Server®. The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

vSphere Client and vCenter Server Management Interface

Instructions in this guide reflect the vSphere Client, an HTML5-based GUI, and the vCenter Server Management Interface. Some additional functions can be performed using the vCenter Server appliance shell and the Direct Console User Interface.

vCenter Server Configuration Overview

vCenter Server is deployed using a preconfigured virtual machine, which is optimized for running VMware vCenter Server® and the associated services.

During the deployment of vCenter Server, you can create a VMware vCenter®Single Sign-On™ domain or join an existing domain. For information about the vCenter Server deployment, see *vCenter Server Installation and Setup*.

vCenter Server is supported on VMware ESXi™ 6.0 and later. The package contains the following software:

- Project Photon OS® 3.0
- PostgreSQL database
- vCenter Server 7.0 and vCenter Server 7.0 components
- Necessary services for running vCenter Server such as vCenter Single Sign-On, License service, and VMware Certificate Authority
  For detailed information about authentication, see *vSphere Authentication*.

Customization of the preconfigured virtual machine is unsupported except for adding memory, CPU, and disk space.

vCenter Server has the following default user names:

- root user with the password that you set during the deployment of the virtual appliance. You use the root user to log in to the vCenter Server Management Interface and to the preconfigured virtual machine operating system.
  Important: The password for the root account of vCenter Server expires after 365 days by default. For information about changing the root password and configuring the password expiration settings, see Change the Password and Password Expiration Settings of the Root User.
- administrator@*your_domain_name* which is the vCenter Single Sign-On user with the password and domain name that you set during the deployment of the appliance.
  When you install vCenter Server, you can change the vSphere domain. Do not use the same domain name as the domain name of your Microsoft Active Directory or OpenLDAP domain name.
  Initially, only the user administrator@*your_domain_name* has the privileges to log in to the vCenter Server system. By default, the administrator@*your_domain_name* user is a member of the SystemConfiguration.Administrators group. This user can add an identity source in which additional users and groups are defined to vCenter Single Sign-On or give permissions to the users and groups. For more information, see *vSphere Security*.

You can configure vCenter Server settings in four ways:

- Use the vCenter Server Management Interface.
  You can edit the system settings such as access, network, time synchronization, and the root password settings. This is the preferred way for configuring vCenter Server.
- Use the vSphere Client.
  You can navigate to the system configuration settings of vCenter Server and join the deployment to an Active Directory domain. You can manage the services that are running in vCenter Server and modify various settings such as access, network, and firewall settings.
- Use the Bash shell.
  You can use TTY1 to log in to the console or can use SSH and run configuration, monitoring, and troubleshooting commands in vCenter Server.
- Use the Direct Console User Interface.
  You can use TTY2 to log in to the vCenter Server Direct Console User Interface to change the password of the root user, configure the network settings, or enable access to the Bash shell or SSH.

What Happened to the Platform Services Controller

In vSphere 7.0, all Platform Services Controller services are consolidated into vCenter Server.

Beginning in vSphere 7.0, deploying or upgrading vCenter Server in vSphere 7.0 requires the use of vCenter Server Appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server Appliance, see the *vSphere Upgrade* documentation.

Using the vCenter Server Management Interface to Configure vCenter Server

After you deploy vCenter Server, you can log in to the vCenter Server Management Interface and edit the settings.

For information about patching vCenter Server and enabling automatic checks for vCenter Server patches, see the *vSphere Upgrade* documentation.

For information backing up and restoring vCenter Server, see *vCenter Server Installation and Setup*.

Log In to the vCenter Server Management Interface

Log in to the vCenter Server Management Interface to access the vCenter Server configuration settings.

Verify that the vCenter Server is successfully deployed and running.

Note: The login session expires if you leave the vCenter Server Management Interface idle for 10 minutes.

1. In a Web browser, go to the vCenter Server Management Interface, https://*`appliance-IP-address-or-FQDN`*:5480.
2. Log in as root.

   The default root password is the password that you set while deploying vCenter Server.

View vCenter ServerHealth Status

You can use the vCenter Server Management Interface to view the overall health status of vCenter Server and health messages.

Log in to the vCenter Server Management Interface as root.

The overall health status of vCenter Server is based on the status of the hardware components such as CPU, memory, database, and storage. It is also based on the update component, which shows whether the software packages are up to date according to the last check for available patches.

Important: If you do not perform regular checks for available patches, the health status of the update component might become out-of-date. For information about how to check for vCenter Server patches and enable automatic checks for vCenter Server patches, see *vSphere Upgrade*.

1. In the vCenter Server Management Interface, click **Summary**.
2. In the Health Status pane, view the Overall Health badge.

Table 128: Health Status

Badge Icon	Description
	Good. All components are healthy.
	Warning. One or more components might become overloaded soon. View the details in the Health Messages pane.
	Alert. One or more components might be degraded. Nonsecurity patches might be available. View the details in the Health Messages pane.
	Critical. One or more components might be in an unusable status and vCenter Server might become unresponsive soon. Security patches might be available. View the details in the Health Messages pane.
	Unknown. No data is available.

Reboot or Shut Down vCenter Server

You can use the vCenter Server Management Interface to restart or power off the virtual machine running.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Summary**.
2. From the top menu pane, click the **Actions** drop-down menu.
3. Click **Reboot** or **Shutdown** to restart or power off the virtual machine.
4. In the confirmation dialog box, click **Yes** to confirm the operation.

Create a Support Bundle

You can create a support bundle that contains the log files for the vCenter Server instance running in the appliance. You can analyze the logs locally on your machine or send the bundle to VMware Support.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Summary**.
2. From the top menu pane, click the **Actions** drop-down menu.
3. Click **Create Support Bundle** and save the bundle on your local machine.

The support bundle is downloaded as a `.tgz` file on your local machine.

Monitor CPU and Memory Use

You can use the vCenter Server Management Interface to monitor the overall CPU and memory use of vCenter Server.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Monitor**.
2. On the Monitor page, click the **CPU & Memory** tab.
3. From the **date range** drop-down menu, select the time period for which you want to generate a CPU utilization trending graph and a memory utilization trending graph.
4. Point to the graphs to see the CPU and memory use for a particular date and time.

Monitor Disk Use

You can use the vCenter Server Management Interface to monitor the disk use of vCenter Server.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Monitor**.
2. On the Monitor page, click the **Disks** tab.

The Monitor Disks pane shows a disk, sortable by name, partition, or utilization.

Monitor Network Use

You can use the vCenter Server Management Interface to monitor the network use of vCenter Server in the last day, week, month, or quarter.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Monitor**.
2. On the Monitor page, click the **Network** tab.
3. From the **date range** drop-down menu, select the time period for generating the network utilization graph.
4. From the table below the graph grid, select a packet or transmit byte rate to monitor.
   The options vary depending on your network settings.
   The network utilization graph refreshes to display the use of the item you select.
5. Point to the network utilization graph to see the network use data for a particular date and time.

Monitor Database Use

You can use the vCenter Server Management Interface to monitor the use of the embedded database of the vCenter Server by data type. You can also monitor space use trending graphs and filter any of the largest data types.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Monitor**.
2. On the Monitor page, click the **Database** tab to monitor the consumed and free space for the vCenter Server database.
3. From the **date range** drop-down menu, select the time period for which you want to generate the space utilization trending graphs.
4. At the base of the graph, click the title a particular database component to include or exclude that component from the graph.

Option	Description
Seat space utilization trend graph	Allows you to select and view alarm, event, task, and stat trendlines.
Overall space utilization trend graph	Allows you to select and view SEAT, DB Log, and core trendlines.

5. Point to the space utilization graph to see the database use value for a particular date and time.

Enable or Disable SSH and Bash Shell Access

You can use the vCenter Server Management Interface to edit the access settings for the appliance.

Log in to the vCenter Server Management Interface as root.

You can enable or disable an SSH administrator login to the appliance. You can also enable access to the vCenter Server Bash shell for a specific time interval.

1. In the vCenter Server Management Interface, click **Access**, and click **Edit**.
2. Edit the access settings for vCenter Server.

Option	Description
Enable SSH login	Enables SSH access to vCenter Server.
Enable DCUI	Enables DCUI access to vCenter Server.
Enable Console CLI	Enables console CLI access to vCenter Server.
Enable Bash Shell	Enables Bash shell access to vCenter Server for the number of minutes that you enter.

3. Click **OK** to save the settings.

Configure the DNS, IP Address, and Proxy Settings

You can set the combination of static and DHCP, IPv4 and IPv6 addresses, edit the DNS settings, and define the proxy settings for vCenter Server.

- To change the IP address of the appliance, verify that the system name of the appliance is an FQDN. The system name is used as a primary network identifier. If you set an IP address as a system name during the deployment of the appliance, you can later change the PNID to an FQDN.
  Note: You can set only IPv4 IP address as system name. The IPv4 IP address must be enabled before this setting.
- To restore a dual stack VC, the base VC after stage 1 deployment should be configured as:
  – If PNID of backed up VC resolves to IPv4 and IPv4 is configured static, the base VC during stage1 should have static or DHCP IPv4 configured.
  – If PNID of backed up VC resolves to IPv4 and IPv4 is configured DHCP, the base VC during stage1 should have DHCP IPv4 configured.
  – If PNID of backed up VC resolves to IPv6 and IPv6 is configured static, the base VC during stage1 should have static or DHCP IPv6 configured.
  – If PNID of backed up VC resolves to IPv6 and IPv6 is configured DHCP, the base VC during stage1 should have DHCP IPv6 configured.
- Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Networking**.
2. From the Network Settings page, click **Edit**.
3. Expand the Hostname and DNS section to configure the DNS settings.

   Note: Valid value for Hostname is either FQDN resolving to enabled IP address or IPv4 IP address.

Option	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.
Enter DNS settings manually	Lets you set the DNS address settings manually. If you select this option, you must provide the following information: • The IP address of the preferred DNS server. • The IP address of the alternate DNS server.

4. From the Network Settings page, click **Edit**.
5. Expand the NIC0 section to configure the gateway settings.

   Note: PNID and network APIs support only NIC0 as primary NIC.

   Recommended steps to configure network other than NIC 0, when vCenter has multiple NICs configured are:

   - NIC 1 is reserved for VCHA and should not be used in multi-NIC configurations.
   - As mentioned in the UI specifications, DGW should be set to NIC 0.
   - As access to vSphere Client is redirected to PNID, only access to NIC 0 is supported or recommended even in multi-NIC configurations.

6. Edit the IPv4 address settings.

Option	Description
Enable or Disable IPv4 settings	Enables or Disables the IPv4 address based on the toggle switch option.
Obtain IPv4 settings automatically	Obtains the IPv4 address for the appliance automatically from the network.

Option	Description
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. You must enter the IP address, subnet prefix length, and the default gateway. **Note:** For static IPv4 or IPv6 addresses, DNS server must be set manually.

Note: Second and third party solutions need to re-register, when there is a change in the IPv4 and IPv6 IP addressess.

7. Edit the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically through DHCP	Assigns IPv6 addresses to the appliance automatically from the network by using DHCP.
Obtain IPv6 settings automatically through router advertisement	Assigns IPv6 addresses to the appliance automatically from the network by using router advertisement.
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1. Click the checkbox. 2. Enter the IPv6 address and the subnet prefix length. 3. Click **Add** to enter additional IPv6 addresses. 4. Click **Save**.

You can configure the appliance to obtain the IPv6 settings automatically through both DHCP and router advertisement. You can assign static a IPv6 address at the same time.

8. To configure a proxy server, in the Proxy Settings section, click **Edit**.
9. Select the proxy setting to enable

Option	Description
HTTPS	Enable to configure the HTTPS proxy settings.
FTP	Enable to configure the FTP proxy settings. **Note:** Ensure that the ICMP is enabled on the proxy server.
HTTP	Enable to configure the HTTP proxy settings.

10. Optional: To add proxy bypass list entries, enter the IPv4 addresses, FQDNs, or domain names that you want to bypass as a comma separated list.
11. Enter the server hostname or IP address.
12. Enter the port.
13. Enter the username (optional).
14. Enter the password (optional).
15. Click **Save**.

Reconfigure the Primary Network Identifier

You can change the FQDN, IP, or PNID of the management network of vCenter Server.

The system name is used as a primary network identifier. If you set an IP address as a system name during the deployment of the appliance, you can later change the PNID to an FQDN. You cannot change an FQDN back to an IP address.

If vCenter High Availability (HA) is enabled, you must deactivate the vCenter HA setup before reconfiguring the PNID.

1. Log in to the vCenter Server Management Interface using your administrator SSO credentials.
2. In the vCenter Server Management Interface, navigate to the **Networking** page and click **Edit**.
3. Select the NIC to be modified and click **Next**.
4. In the **Edit Settings** pane, change the host name and provide the new IP address. Click **Next**.
5. In the **SSO Credentials** pane, provide the administrator SSO credentials. You must use `administrator@<domain_name>` credentials.
6. In the **Ready to Complete** pane, review your new settings and check the backup acknowledgement box. Click **Finish**.

   A taskbar shows the status of the network update. To cancel the update, click **Cancel Network Update**. When the network reconfiguration is complete, the UI redirects to the new IP address.
7. To finish the reconfiguration process and restart services, log in using your administrator SSO credentials.
8. On the **Networking** page, verify the new host name and IP address.

- Re-register all deployed plug-ins.
- Regenerate all custom certificates.
- If vCenter HA was enabled, reconfigure vCenter HA.
- If Active Domain was enabled, reconfigure Active Domain.
- If Hybrid Link mode was enabled, reconfigure Hybrid Link with the Cloud vCenter Server.

Edit the Firewall Settings

After you deploy vCenter Server, you can edit its firewall settings and create firewall rules using the Management Interface.

Verify that the user who logs in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in vCenter Single Sign-On.

You can set up firewall rules to accept or block traffic between vCenter Server and specific servers, hosts, or virtual machines. You cannot block specific ports, you block all the traffic.

1. In the vCenter Server Management Interface, click **Firewall**.
2. Edit the firewall settings.

Command	Action
Add	1. To create a firewall rule, click **Add**. 2. Select a network interface of the virtual machine. 3. Enter the IP address of the network to apply this rule to. The IP address can be IPv4 and IPv6 address. 4. Enter a subnet prefix length. If you only block one IP address, use a 32-bit subnet mask. 5. From the **Action** drop-down menu, select whether to **Accept**, **Ignore**, **Reject**, or **Return** the connection between vCenter Server and the network that you entered. 6. Click **Save**.
Edit	1. Select a rule and click **Edit**. 2. Edit the settings of the rule. 3. Click **Save**.
Delete	1. Select a rule and click **Delete**. 2. At the prompt, click **Delete** again.
Reorder	1. Select a rule and click **Reorder**.

Command	Action
	2. In the Reorder pane, select the rule to move. 3. Click **Move Up** or **Move Down**. 4. Click **Save**.

Configure the System Time Zone and Time Synchronization Settings

After you deploy vCenter Server, you can change the system time zone and time synchronization settings from the vCenter Server Management Interface.

Log in to the vCenter Server Management Interface as root.

When you deploy vCenter Server, you either use the time settings of the ESXi host on which vCenter Server is running or you configure the time synchronization based on an NTP server. If the time settings in your vSphere network change, you can edit the time zone and time synchronization settings in the appliance.

1. In the vCenter Server Management Interface, click **Time**.
2. Configure the system time zone settings.
   a) In the Time zone pane, click **Edit**.
   b) From the **Time zone** drop-down menu, select a location or time zone and click **Save**.
3. Configure the time synchronization settings.
   a) In the Time synchronization pane, click **Edit**.
   b) From the **Mode** drop-down menu, configure the time synchronization method.

Option	Description
Disabled	No time synchronization. Uses the system time zone settings.
Host	Enables VMware Tools time synchronization. Uses VMware Tools to synchronize the time of the appliance with the time of the ESXi host.
NTP	Enables NTP synchronization. You must enter the IP address or FQDN of one or more NTP servers.

   c) Click **Save**.

Start, Stop, and Restart Services

You can use the vCenter Server Management Interface to view the status of vCenter Server components and to start, stop, and restart services.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Services**.

   The Services page displays a table of the installed services that can be sorted by name, startup type, health, and state.
2. Select a service and click **SET STARTUP TYPE** to configure either Manual or Automatic start of a service.
3. Select a service and click **START** to start a service.
4. Select a service and clilck **STOP** to stop, or **RESTART** to restart a service, then click **OK**.

   Warning: Stopping or Restarting some services may lead to functionality becoming temporarily unavailable.

Configure Update Settings

You can use the vCenter Server Management Interface to configure your update settings and check for new updates.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Update**.
2. To configure your update settings, click **Settings**.
   a) To check for updates automatically, select the checkbox.
   b) Select to use a default or custom repository.
   c) If you selected a custom repository, enter the repository URL, username (optional), and password (optional). Click **Save**.
      For the URL, HTTPS and FTPS protocols are supported.
3. To manually check for updates, click the **Check Updates** drop-down menu.
   a) Select to check a **CD-ROM** or a **CD-ROM + URL** for updates.

The Available Updates table displays available updates sortable by version, type, release date, reboot requirement, and severity.

Change the Password and Password Expiration Settings of the Root User

When you deploy vCenter Server, you set the initial password of the root user, which expires after 90 days by default. You can change the root password and the password expiration settings from the vCenter Server Management Interface.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Administration**.
2. In the Password section, click **Change**.
3. Enter the current password and the new password, then click **Save**.
4. Configure the password expiration settings for the root user.
   a) In the Password expiration settings section, click **Edit** and select the password expiration policy.

Option	Description
Yes	The password of the root user expires after a specified number of days. You must provide the following information: • **Root password validity (days)** The number of days after which the password expires. • **Email for expiration warning** The email address to which vCenter Server sends a warning message before the expiration date.
No	The password of the root user never expires.

   b) In the Password expiration settings pane, click **Save** to apply the new password expiration settings.
   The Password expiration settings section displays the new expiration date.

Forward vCenter Server Log Files to Remote Syslog Server

You can forward the vCenter Server log files to a remote syslog server to conduct an analysis of your logs.

Log in to the vCenter Server Management Interface as root.

Note: ESXi can be configured to send log files to a vCenter Server rather than storing them to a local disk. The recommended maximum numbers of supported hosts to collect logs from is 30. See http://kb.vmware.com/s/article/2003322 for information on how to configure ESXi log forwarding. This feature is intended for smaller environments

with stateless ESXi hosts. For all other cases, use a dedicated log server. Using vCenter Server to receive ESXi log files might impact vCenter Server performance.

1. In the vCenter Server Management Interface, select **Syslog**.
2. In the Forwarding Configuration section, click **Configure** if you have not configured any remote syslog hosts. Click **Edit** if you already have configured hosts.
3. In the Create Forwarding Configuration pane, enter the server address of the destination host. The maximum number of supported destination hosts is three.
4. From the **Protocol** drop-down menu, select the protocol to use.

Menu Item	Description
TLS	Transport Layer Security
TCP	Transmission Control Protocol
RELP	Reliable Event Logging Protocol
UDP	User Datagram Protocol

5. In the **Port** text box, enter the port number to use for communication with the destination host.
6. In the Create Forwarding Configuration pane, click **Add** to enter another remote syslog server.
7. Click **Save**.
8. Verify that the remote syslog server is receiving messages.
9. In the Forwarding Configuration section, click **Send Test Message.**
10. Verify on the remote syslog server that the test message was received.

    The new configuration settings are shown in the Forwarding Configuration section.

Configure and Schedule Backups

You can use the vCenter Server Management Interface to set a backup location, create a backup schedule, and monitor backup activity.

Log in to the vCenter Server Management Interface as root.

1. In the vCenter Server Management Interface, click **Backup**.
2. To create a backup schedule, click **Configure**. To edit an existing backup schedule, click **Edit**.
   a) In the **Backup Schedule** pane, enter the backup location using the format `protocol://server-address<:port-number>/folder/subfolder`.

      Supported protocols for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB, and HTTP.
   b) Enter the username and password for the backup server.
   c) Enter the time and frequency for the backup to occur.
   d) (Optional) Enter an encryption password for the backup.
   e) Indicate the number of backups to retain.
   f) Indicate the types of data to be backed up.
3. To initiate a manual backup, click **Backup Now**.

Information for scheduled and manual backups is displayed in the **Activity** table.

Using the vSphere Client to Configure vCenter Server

You can perform some configuration operations from the vSphere Client such as joining the appliance to an Active Directory domain, networking, and other settings.

Configuring vCenter Server

You can configure vCenter Server from the vSphere Client and from the vSphere Web Client.

What you can do depends on your deployment.

On-premises vCenter Server	You can change many of the vCenter Server settings, including licensing, statistics collection, logging, and more.
vCenter Server in VMware Cloud on AWS	VMware preconfigures vCenter Server instances when you create an SDDC. You can view configuration settings and advanced settings, and you can set a Message of the Day.

Configure License Settings for vCenter Server

You must assign a license to a vCenter Server system before its evaluation period expires or its currently assigned license expires. If you upgrade, combine, or divide vCenter Server licenses in Customer Connect, you must assign the new licenses to vCenter Server systems and remove the old licenses.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **Licensing**.
4. Click **Assign License**.
5. In the **Assign License** dialog box, select the task that you want to perform.
   - In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
----------	**----------**
Select a newly created license	1. Click the **New License** tab. 2. In the **Assign License** dialog box, type or copy and paste a license key and click **OK**. 3. Enter a name for the new license and click **OK**. Details about the product, product features, capacity, and expiration period appear on the page. 4. Click **OK**. 5. In the **Assign License** dialog box, select the newly created license, and click **OK**.

The license is assigned to the vCenter Server system, and one instance from the license capacity is allocated for the vCenter Server system.

Configuring Statistics Settings

To set up how statistical data is recorded, you configure collection intervals for statistics. You can access the stored statistical information through command-line monitoring utilities or by viewing performance charts in the vSphere Client.

Configure Statistics Collection Intervals in the vSphere Client

Statistic collection intervals determine the frequency at which statistic queries occur, the length of time statistical data is stored in the database, and the type of statistical data that is collected. You can view the collected statistics through the performance charts in the vSphere Client or through command-line monitoring utilities.

Required privilege: **Performance** > **ModifyIntervals**

Note: Not all interval attributes are configurable.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. To enable or disable a statistics interval, check the box for that interval.
6. To change a statistics interval attribute value, select a value from the drop-down menu.
   a) In **Interval Duration**, select the time interval in which statistics data is collected.
   b) In **Save For**, select for how long the archived statistics are kept in the database.
   c) In **Statistics Level**, select a new level for collecting statistics.

      The lower the level is, the fewer number of statistic counters are used. Level 4 uses all statistics counters. Use it only for debugging purposes.

      The statistics level must be less than or equal to the statistics level that is set for the preceding statistics interval. This requirement is a vCenter Server dependency.
7. Optional: In Database Size, estimate the effect of the statistics settings on the database.
   a) Enter the number of **Physical Hosts**.
   b) Enter the number of **Virtual Machines**.

      The estimated space required and number of database rows required are calculated and displayed.
   c) If necessary, make changes to your statistics collection settings.
8. Click **Save**.

   Relationships Between the Default Settings for Statistics Intervals

   - Samples that are collected every 5 minutes are stored for 1 day.
   - Samples that are collected every 30 minutes are stored for 1 week.
   - Samples that are collected every 2 hours are stored for 1 month.
   - Samples that are collected on 1 day are stored for 1 year.

   For all statistics intervals, the default level is 1. It uses the Cluster Services, CPU, Disk, Memory, Network, System, and Virtual Machine Operations counters.

Data Collection Levels

Each collection interval has a default collection level that determines the amount of data gathered and which counters are available for display in the charts. Collection levels are also referred to as statistics levels.

Table 129: Statistics Levels

Level	Metrics	Best Practice
Level 1	• Cluster Services (VMware Distributed Resource Scheduler) – all metrics • CPU – cpuentitlement, totalmhz, usage (average), usagemhz • Disk – capacity, maxTotalLatency, provisioned, unshared, usage (average), used • Memory – consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon), totalbandwidth (DRAM or PMem) • Network – usage (average), IPv6 • System – heartbeat, uptime • Virtual Machine Operations – numChangeDS, numChangeHost, numChangeHostDS	Use for long-term performance monitoring when device statistics are not required. Level 1 is the default Collection Level for all Collection Intervals.
Level 2	• Level 1 metrics • CPU – idle, reservedCapacity • Disk – All metrics, excluding numberRead and numberWrite. • Memory – All metrics, excluding memUsed, maximum and minimum rollup values, read or write latency (DRAM or PMem). • Virtual Machine Operations – All metrics	Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.
Level 3	• Level 1 and Level 2 metrics • Metrics for all counters, excluding minimum and maximum rollup values. • Device metrics	Use for short-term performance monitoring after encountering problems or when device statistics are required.
Level 4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	Use for short-term performance monitoring after encountering problems or when device statistics are required.

Note:

When the statistics levels, level 3 or level 4 are used beyond the default value, it may cause one particular process, vpxd, to sustain memory growth, if it cannot save the statistics information to the database as quickly as required. If the usage limit of these statistics levels is not monitored closely, it may cause vpxd to grow out of memory and eventually crash.

So, in case the administrator decides to elevate any of these levels, it is necessary for the administrator to monitor the size of the vpxd process to make sure that is not growing boundlessly after the change.

Configure Runtime Settings for vCenter Server

You can change the vCenter Server ID, managed address, and name. You might need to make changes if you run multiple vCenter Server systems in the same environment.

Required privilege: **Global** > **Settings**

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. In the Edit vCenter Server Settings dialog box, select **Runtime Settings**.
6. In **vCenter Server unique ID**, enter a unique ID.

   You can change this value to a number from 0 through 63 to identify each vCenter Server system running in a common environment. By default, an ID value is generated randomly.
7. In **vCenter Server managed address**, enter the vCenter Server system address.

   The address can be IPv4, IPv6, a fully qualified domain name, an IP address, or another address format.
8. In **vCenter Server name**, enter the name of the vCenter Server system.

   If you change the DNS name of the vCenter Server, you can use this text box to modify the vCenter Server name to match.
9. Click **Save**.

If you made changes to the vCenter Server system unique ID, you must restart the vCenter Server system for these changes to take effect.

Configure User Directory Settings

You can configure some of the ways vCenter Server interacts with the user directory server that is configured as an identity source.

Required privilege: **Global** > **Settings**

For vCenter Server versions before vCenter Server 5.0, these settings apply to an Active Directory associated with vCenter Server. For vCenter Server 5.0 and later, these settings apply to vCenter Single Sign-On identity sources.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. In the Edit vCenter general settings window, select **User directory**.
6. In **User directory timeout**, type the timeout interval in seconds for connecting to the directory server.
7. Enable the **Query Limit** box to set a query limit size.
8. In **Query Limit Size**, enter the number of users and groups for which you can associate permissions on the child inventory objects of the vCenter Server system.

   Note: You can associate permissions with users and groups from the Add Permissions dialog box that displays when you click **Add permissions** in **Manage** > **Permissions** for a vSphere inventory object.

9. Click **SAVE**.

Configure Mail Sender Settings

You must configure the email address of the sender account to use vCenter Server operations, such as sending email notifications as alarm actions. You can send email alerts and alarms using either anonymous or authentication mode.

Required privilege: **Global** > **Settings**

SMTP authentication is available for:

- vSphere 7.0 Update 1 and later versions only.
- Office 365 mailbox users only.
- SMTP mail sender should meet the basic requirements for SMTP Authentication as mentioned in Microsoft's document Requirement for SMTP AUTH client submission.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **Mail** and enter the settings that vCenter Server uses to send email alerts.
6. In **Mail server** text box, enter the SMTP server information.
   The SMTP server is the DNS name or IP address of the SMTP gateway to use for sending email messages.
   - For sending mails anonymously, you can enter any SMTP server information as the mail server name.
   - For SMTP authentication, you must enter the mail server name as `smtp.office365.com` , unless you have some customized configuration. Do not use IP address as mail server as IP address is not supported for SMTP authentication.
7. In **Mail sender** text box, enter the sender account information.
   The sender account is the email address of the sender.
   For SMTP authentication, you must enter a valid SMTP account name in the **Mail sender** text box.

   Note: You must enter the full email address, including the domain name.

   For example, *`mail_server@example.com`*
8. Click **SAVE**.
9. This step is applicable only for SMTP authentication.
   You must configure the SMTP user settings as below:
   1. Select the **Configure** tab.
   2. Select **Advanced Settings**.
   3. Click **EDIT SETTINGS** and enter the following values for the configuration parameters:

Name	Value
`mail.smtp.username`	SMTP account name.
`mail.smtp.password`	SMTP account password. **Note:** Currently, the account password is not masked and is visible. You must use a dedicated SMTP mail user until the masking is available in upcoming releases.

Name	Value
mail.smtp.port	587

4. Click **SAVE**.

You can perform the following steps to test the mail settings:

1. Create an alarm that is triggered by a user action.
   For example, the user action can be powering off a virtual machine.
2. Verify that you receive an email, when the alarm is triggered.

Configure SNMP Settings

You can configure up to four receivers to receive SNMP traps from vCenter Server. For each receiver, specify a host name, port, and community.

Required privilege: **Global** > **Settings**

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **SNMP receivers**.
6. Select the **Enable receiver 1** box.
7. In **Primary Receiver URL**, enter the host name or IP address of the SNMP receiver.
8. In **Receiver port**, enter the port number of the receiver.
   The port number must be a value between 1 and 65535.
9. In **Community string**, enter the community identifier.
10. To send alarms to multiple receivers, select the additional **Enable receiver** boxes and enter the host name, port number, and community identifier for those receivers.
11. Click **Save**.

View Port Settings

You can view the ports used by the Web service to communicate with other applications. You cannot configure these port settings.

The Web service is installed as part of the VMware vCenter Server installation. The Web service is a required component for third-party applications that use the VMware SDK application programming interface (API). For information about installing the Web service, see the *vCenter Server Installation and Setup* documentation.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **Ports**.
   The ports used by the Web service are displayed.

6. Click **Save**.

Configure Timeout Settings

You can configure the timeout intervals for vCenter Server operations. These intervals specify the amount of time after which the vSphere Client times out.

Required privilege: **Global** > **Settings**

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **Timeout settings**.
6. In **Normal**, type the timeout interval in seconds for normal operations.
   Do not set the value to zero (0).
7. In **Long**, enter the timeout interval in minutes for long operations.
   Do not set the value to zero (0).
8. Click **Save**.
9. Restart the vCenter Server system for the changes to take effect.

Configure Logging Options

You can configure the amount of detail that vCenter Server collects in log files.

Required privilege: **Global** > **Settings**

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **Logging settings**.
6. Select the logging options.

Option	Description
None	Turns off logging
Error	Displays only error log entries
Warning	Displays warning and error log entries
Info	Displays information, error, and warning log entries
Verbose	Displays information, error, warning, and verbose log entries
Trivia	Displays information, error, warning, verbose, and trivia log entries

7. Click **SAVE**.

Changes to the logging settings take effect immediately. You do not need to restart the vCenter Server system.

Configure Database Settings

You can configure the maximum number of database connections that can occur simultaneously. To limit the growth of the vCenter Server database and save storage space, you can configure the database to discard information about tasks or events periodically.

Note: Do not use the database retention options, if you want to keep a complete history of tasks and events for your vCenter Server.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. In Edit vCenter general settings window, click **Database**.
6. In **Maximum connections** field, enter the required number of connections.

   Note: Do not change this value unless one of these issues exists in your system.

   - If your vCenter Server system performs many operations frequently and performance is critical, increase the number of connections.
   - If the database is shared and connections to the database are costly, decrease the number of connections.
7. Enable **Task cleanup** option for vCenter Server to delete the retained tasks periodically.
8. Optional: In **Task retention (days)** field, enter a value (in days).

   Information about tasks that are performed on this vCenter Server system is discarded after the specified number of days.
9. Enable **Event cleanup** option for vCenter Server to clean up the retained events periodically.
10. Optional: In **Event retention (days)** field, enter a value (in days).

    Information about events for this vCenter Server system is discarded after the specified number of days.

    Note: Monitor vCenter Server database consumption and disk partition in the vCenter Server Management Interface.

    Warning: Increasing the events retention to more than 30 days results in significant increase of vCenter database size and can shutdown the vCenter Server. Ensure that you increase the vCenter database accordingly.

11. Restart the vCenter Server to apply changes manually.
12. Click **SAVE**.

Verifying SSL Certificates for Legacy Hosts

You can configure vCenter Server to check the SSL certificates of hosts to which it connects. If you configure this setting, vCenter Server and the vSphere Client check for valid SSL certificates before connecting to a host for operations such as adding a host or making a remote console connection to a virtual machine.

vCenter Server 5.1 and vCenter Server 5.5 always connect to ESXi hosts using SSL thumbprint certificates. Starting with vCenter Server 6.0, the SSL certificates are signed by VMware Certificate Authority by default. You can instead use certificates from a third-party CA. Thumbprint mode is supported only for legacy hosts.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **SSL settings**.
6. Determine the host thumbprint for each legacy host that requires validation.
   a) Log in to the direct console.
   b) Select **View Support Information** on the **System Customization** menu.
      The thumbprint is displayed in the column on the right.
7. Compare the thumbprint you obtained from the host with the thumbprint listed in the vCenter Server SSL settings dialog box.
8. If the thumbprints match, select the check box for the host.
   Hosts that are not selected will be disconnected after you click **Save**.
9. Click **Save**.

Configure Advanced Settings

In **Advanced Settings**, you can modify the vCenter Server configuration file, `vpxd.cfg`.

Required privilege: **Global** > **Settings**

You can use **Advanced Settings** to add entries to the `vpxd.cfg` file, but not to edit or delete them. VMware recommends that you change these settings only when instructed to do so by VMware technical support or when you are following specific instructions in VMware documentation.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Select **Advanced Settings**.
4. Click **Edit Settings**.
5. In the **Name** field, type a name for the setting. Names must start with 'config.' For example: `config.log`.
6. In the **Value** field, type the value for the specified setting.
7. Click **Add**.
8. Click **Save**.

Newly added advanced settings have `config.` appended to the setting keys in the `vpxd.cfg` file. For example:

```
config.example.setting = exampleValue
```

Many advanced settings changes require you to restart the vCenter Server system. Consult VMware technical support to determine if your changes require a restart.

Send a Message to Other Logged In Users

Administrators can send messages to users who are currently logged in to a vCenter Server system. The message might announce maintenance or ask users to log out temporarily.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Click **Configure**.
3. Select **Settings** > **Message of the Day** and click **Edit**.
4. Enter a message and click **OK**.

The message appears at the top of the vSphere Client in each active user session.

Join or Leave an Active Directory Domain

You can join vCenter Server to an Active Directory domain. You can attach the users and groups from this Active Directory domain to your vCenter Single Sign-On domain. You can leave the Active Directory domain.

- Verify that the user who logs in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in vCenter Single Sign-On.
- Verify that the system name of the appliance is an FQDN. If, during the deployment of the appliance, you set an IP address as a system name, you cannot join vCenter Server to an Active Directory domain.

Important: Joining vCenter Server to an Active Directory domain with a read-only domain controller (RODC) is not supported. You can join vCenter Server only to an Active Directory domain with a writable domain controller.

If you want to configure permissions so that users and groups from an Active Directory can access the vCenter Server components, you must join the vCenter Server instance to the Active Directory domain.

For example, to enable an Active Directory user to log in to the vCenter Server instance by using the vSphere Client, you must join the vCenter Server instance to the Active Directory domain and assign the Administrator role to this user.

1. Use the vSphere Client to log in as administrator@*your_domain_name* to the vCenter Server instance.
2. From the vSphere Client menu, select **Administration**.
3. Select **Single Sign On** > **Configuration**.
4. Click on the **Identity Provider** tab, and select **Active Directory Domain** as the identity provide type.
5. Click **JOIN AD**.
6. In the Join Active Directory Domain window, provide the following details.

Option	Description
Domain	Active Directory domain name, for example, mydomain.com. Do not provide an IP address in this text box.
Organization Unit (optional)	The full Organization Unit (OU) LDAP FQDN, for example, OU=Engineering,DC=mydomain,DC=com. **Important:** Use this text box only if you are familiar with LDAP.
Username	User name in User Principal Name (UPN) format, for example, jchin@mydomain.com. **Important:** Down-level login name format, for example, DOMAIN\UserName, is unsupported.
Password	Password of the user.

   Note: Reboot the node to apply changes.
7. Click **JOIN** to join the vCenter Server to the Active Directory domain.
   The operation silently succeeds and you can see the Join AD option turned to Leave AD.
8. Optional: To leave the Active Directory Domain, click **LEAVE AD**.
9. Restart the vCenter Server to apply the changes.

   Important: If you do not restart the vCenter Server, you might encounter problems when using the vSphere Client.
10. Select **Identity Sources** tab, and click the **ADD**.
    1. In the Add Identity Source window, select **Active Directory (Integrated Windows Authentication)** as the Identity Source Type.
    2. Enter the identity source settings of the joined Active Directory domain, and click **ADD**.

Table 130: Add Identity Source Settings

Text Box	Description
Domain name	FDQN of the domain. Do not provide an IP address in this text box.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.
Use Service Principal Name (SPN)	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.

Text Box	Description
Service principal name	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, STS/example.com. You might have to run `setspn -S` to add the user you want to use. See the Microsoft documentation for information on `setspn`. The SPN must be unique across the domain. Running `setspn -S` checks that no duplicate is created.
Username	Name of a user who can authenticate with this identity source. Use the email address format, for example, jchin@mydomain.com. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).
Password	Password for the user who is used to authenticate with this identity source, which is the user who is specified in User Principal Name. Include the domain name, for example, jdoe@example.com.

On the **Identity Sources** tab, you can see the joined Active Directory domain.
You can configure permissions so that users and groups from the joined Active Directory domain can access the vCenter Server components. For information about managing permissions, see the *vSphere Security* documentation.

Add a User to the SystemConfiguration.BashShellAdministrators Group

To enable access to the appliance Bash shell by using the vSphere Client, the user you use to log in must be a member of the SystemConfiguration.BashShellAdministrators group. By default, this group is empty and you must add a user to the group manually.

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

1. Use the vSphere Client to log in as administrator@*`your_domain_name`* to the vCenter Server instance.
   The address is of the type http://*`appliance-IP-address-or-FQDN`*/ui.
2. From the vSphere Client menu, select **Administration**.
3. Select **Single Sign On** > **Users and Groups**.
4. Click on the **Groups** tab, select **SystemConfiguration.BashShellAdministrators** from the options available in the Group Name column.
5. Click **EDIT**.
6. In the **Edit Group** window, to add members, select the domain from the dropdown menu and then search for the required users.
7. Click **SAVE**.

Reboot a Node

In the vSphere Client, you can reboot a node in vCenter Server.

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

1. Use the vSphere Client to log in as administrator@*your_domain_name* to the vCenter Server instance.
2. On the vSphere Client main page, click **Administration** > **Deployment** > **System Configuration**.
3. Under System Configuration, select a node from the list.
4. Click **REBOOT NODE**.

View the Health Status of Nodes

In the vSphere Client, you can view the health status of vCenter Server nodes.

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

vCenter Server instances and machines that run vCenter Server services are considered nodes. Graphical badges represent the health status of nodes.

1. Use the vSphere Client to log in as administrator@*your_domain_name* to the vCenter Server instance.
   The address is of the type http://*appliance-IP-address-or-FQDN*/ui.
2. From the vSphere Client menu, select **Administration**.
3. Select **Deployment** > **System Configuration**.
4. Select a node to view its health status.

Table 131: Health States

Badge Icon	Description
	Good. The health of the object is normal.
	Warning. The object is experiencing some problems.
	Critical. The object is either not functioning properly or will stop functioning soon.
	Unknown. No data is available for this object.

Export a Support Bundle

You can export a support bundle containing the log files for a specific product included in vCenter Server.

Verify that the user who logs in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in vCenter Single Sign-On.

1. Use the vSphere Client to log in as administrator@*your_domain_name* to the vCenter Server instance.
   The address is of the type http://*appliance-IP-address-or-FQDN*/ui.

2. On the vSphere Client home page, click **Administration** > **Deployment** > **System Configuration**.
3. Select a node from the list and click **Export Support Bundle**.
4. In the **Export Support Bundle** window, expand the trees to view the services running in the appliance and deselect the services for which you do not want to export log files.

   All the services are selected by default. If you want to export the support bundle and send it to VMware Support, leave all check boxes selected. The services are separated in two categories: a Cloud infrastructure category, which contains the services of specific products in the appliance, and a Virtual appliance category, which contains the services specific for the appliance and the vCenter Server product.
5. Click **Export Support Bundle** and save the bundle on your local machine.

You saved the support bundle to your machine and can explore it.

Using the Appliance Shell to Configure vCenter Server

You can access all of the vCenter Server API commands and plug-ins that you can use for monitoring, troubleshooting, and configuring the appliance by using the appliance shell.

You can run all commands in the appliance shell with or without the `pi` keyword.

Access the Appliance Shell

To access the plug-ins included in the appliance shell and to be able to see and use the API commands, first access the appliance shell.

1. Access the appliance shell.
   - If you have direct access to the appliance console, press Alt+F1.
   - If you want to connect remotely, use SSH or another remote console connection to start a session to the appliance.
2. Enter a user name and password recognized by the appliance.

You are logged in to the appliance shell and can see the welcome message.

Enable and Access the Bash Shell from the Appliance Shell

If you log in to the appliance shell as a user who has a super administrator role, you can enable access to the Bash shell of the appliance for other users. The root user has access to the appliance Bash shell by default.

The appliance Bash shell is enabled by default for the root

1. Access the appliance shell and log in as a user who has a super administrator role.

   The default user with a super administrator role is root.
2. If you want to enable the Bash shell access for other users, run the following command.

   ```
   shell.set --enabled true
   ```
3. To access the Bash shell run `shell` or `pi shell`.

Keyboard Shortcuts for Editing Commands

You can use various keyboard shortcuts to enter and edit commands in the appliance Bash shell.

Table 132: Keyboard Shortcuts and Function

Keyboard Shortcut	Details
Tab	Completes the current command. If you enter a part of the command name and press the Tab key, the system completes the command name. To view the commands that match a set of characters that you enter, type a character and press the Tab key.
Enter (at the command line)	Runs the command that you entered.
Enter (at the **More** prompt)	Displays the next page of output.
Delete or Backspace	Deletes the character that is on the left of the cursor.
Left arrow or Ctrl+B	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys to go back to the beginning of the command.
Right arrow or Ctrl+F	Moves the cursor one character to the right.
Esc, B	Moves the cursor one word back.
Esc, F	Moves the cursor one word forward.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+D	Deletes the character selected by the cursor.
Ctrl+W	Deletes the word next to the cursor.
Ctrl+K	Deletes the line forward. When you press Ctrl+K, everything that you entered starting from the cursor location to the end of the command line is deleted.
Ctrl+U or Ctrl+X	Deletes the line backward. When you press Ctrl+U, everything from the beginning of the command line to the cursor location is deleted.
Ctrl+T	Changes the places of the character to the left of the cursor with the character selected by the cursor.
Ctrl+R or Ctrl+L	Displays the system prompt and command line.
Ctrl+V or Esc, Q	Inserts a code to indicate to the system that the following keystroke must be treated as a command entry, not as an editing key.
Up arrow, or Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command.
Down arrow or Ctrl+N	Returns to more recent commands in the history buffer after you use the Up arrow or Ctrl+P to recall commands.
Ctrl+Y	Recalls the most recent entry in the delete buffer. The delete buffer contains the last 10 items you have cut or deleted.
Esc, Y	Recalls the next entry in the delete buffer. The delete buffer contains the last 10 items you have cut or deleted. Press Ctrl+Y first to recall the most recent entry, and then press Esc, Y up to nine times to recall the remaining entries in the buffer.
Esc, C	Capitalizes the character selected by the cursor.
Esc, U	Changes the casing for all characters in the word selected by the cursor, up to the next space, to uppercase.
Esc, L	Changes the capitalized letters in a word from the character selected by the cursor to the end of the word to lowercase.

Get Help About the Plug-Ins and API Commands in the Appliance

You can access the vCenter Server plug-ins and API commands from the appliance shell. You can use the plug-ins and commands for monitoring, troubleshooting, and configuring the appliance.

You can use the Tab key to autocomplete API commands, plug-in names, and API parameters. Plug-in parameters do not support autocompletion.

1. Access the appliance shell and log in.
2. To get help about the plug-ins, run the `help pi list` or the `? pi list` command.
   You receive a list with all the plug-ins in the appliance.
3. To get help about the API commands, run the `help api list` or the `? api list` command.
   You receive a list with all the API commands in the appliance.
4. To get help about a particular API command, run the `help api` *`api_name`* or the `? api` *`api_name`* command. For example, to receive help about the `com.vmware.appliance.version1.timesync.set` command, run `help api timesync.set` or `? api timesync.set`.

Plug-Ins in the vCenter Server Shell

The plug-ins in vCenter Server provide you with access to various administrative tools. The plug-ins reside in the CLI itself. The plug-ins are standalone Linux or VMware utilities, which do not depend on any VMware service.

Table 133: Plug-Ins Available in the vCenter Server

Plug-In	Description
`com.vmware.clear`	A plug-in that you can use to clear the terminal screen.
`com.vmware.cmsso-util`	A plug-in that you use for orchestrating changes to PNID, Machine Certificate, unregistering a node from Component Manager, vCenter Single Sign-On, and reconfiguring vCenter Server.
`com.vmware.dcli`	vAPI based CLI client.
`com.vmware.nslookup`	A plug-in that you can use to query the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
`com.vmware.pgrep`	A plug-in that you can use to search for all named processes.
`com.vmware.pgtop`	A plug-in that you can use to monitor the PostgreSQL database.
`com.vmware.ping`	A plug-in that you can use to ping a remote host. Accepts the same arguments as bin/ping.
`com.vmware.ping6`	A plug-in that you can use to ping a remote host. Accepts the same arguments as bin/ping6.
`com.vmware.portaccess`	A plug-in that you can use to troubleshoot the port access of a host.
`com.vmware.ps`	A plug-in that you can use to see statistics on running processes.
`com.vmware.rvc`	Ruby vSphere Console
`com.vmware.service-control`	A plug-in that you can use to manage VMware services.
`com.vmware.shell`	A plug-in that allows access to the appliance Bash shell.
`com.vmware.showlog`	A plug-in that you can use to browse the log files.

Plug-In	Description
com.vmware.shutdown	A plug-in that you can use to restart or power off the appliance.
com.vmware.software-packages	A plug-in that you can use to update the software packages in the appliance.
com.vmware.support-bundle	A plug-in that you can use to create a bundle on the local file system and export it to a remote Linux system. If you use the plug-in with the `stream` command, the support bundle is not created on the local file system, but is directly exported to the remote Linux system.
com.vmware.top	A plug-in that displays process information. Accepts the same arguments as /usr/bin/top/.
com.vmware.tracepath	A plug-in that traces the path to a network host. Accepts the same arguments as /sbin/tracepath.
com.vmware.tracepath6	A plug-in that traces the path to a network host. Accepts the same arguments as /sbin/tracepath6.
com.vmware.updatemgr-util	A plug-in that you can use to configure VMware Update Manager.
com.vmware.vcenter-restore	A plug-in that you can use to restore vCenter Server.
com.vmware.vimtop	A plug-in that you can use to view a list of vSphere services and their resource use.

Browse the Log Files By Using the showlog Plug-In

You can browse the log files in vCenter Serverto examine them for errors.

1. Access the appliance shell and log in.
2. Type the `showlog` command, add a space, and press the Tab key to view all the contents of the `/var/log` folder.
3. Run the command for viewing the firstboot log files.

```
showlog /var/log/firstboot/cloudvm.log
```

API Commands in the Appliance Shell

The API commands in vCenter Server let you perform various administrative tasks. The API commands are provided by appliance management service. You can edit time synchronization settings, monitor processes and services, set up the SNMP settings, and so on.

Table 134: API Commands Available in vCenter Server

API Command	Description
com.vmware.appliance.health.applmgmt.get	Get the health of the applmgmt service.
com.vmware.appliance.health.databasestorage.get	Get the health of the database storage.
com.vmware.appliance.health.load.get	Get the CPU load health.
com.vmware.appliance.health.mem.get	Get the memory health.
com.vmware.appliance.health.softwarepackages.get	Get the health of the system update.
com.vmware.appliance.health.storage.get	Get the overall storage health.
com.vmware.appliance.health.swap.get	Get the swap health.

API Command	Description
com.vmware.appliance.health.system.get	Get the system health.
com.vmware.appliance.health.system.lastcheck	Get the time of the last check of the health status.
com.vmware.appliance.monitoring.list	Get a list of monitored items.
com.vmware.appliance.monitoring.get	Get monitored item information.
com.vmware.appliance.monitoring.query	Query a range of values for the monitored items.
com.vmware.appliance.recovery.backup.job.cancel	Cancel a backup job by id.
com.vmware.appliance.recovery.backup.job.create	Start a backup job.
com.vmware.appliance.recovery.backup.job.get	Get a status of the backup job by id.
com.vmware.appliance.recovery.backup.job.list	Get a list of backup jobs.
com.vmware.appliance.recovery.backup.parts.list	Get a list of the vCenter Server components that can be included in a backup job.
com.vmware.appliance.recovery.backup.parts.get	Get detailed info for a backup part.
com.vmware.appliance.recovery.backup.validate	Validate parameters for a backup job without starting the job.
com.vmware.appliance.recovery.restore.job.cancel	Cancel a restore job.
com.vmware.appliance.recovery.restore.job.create	Start a restore job.
com.vmware.appliance.recovery.restore.job.get	Get status of the restore job.
com.vmware.appliance.recovery.restore.validate	Validate restore parameters of a restore job without starting the job.
com.vmware.appliance.system.uptime.get	Gets the system uptime.
com.vmware.appliance.version1.access.consolecli.get	Get information about the state of the console-based controlled CLI (TTY1).
com.vmware.appliance.version1.access.consolecli.set	Set enabled state of console-based controlled CLI (TTY1).
com.vmware.appliance.version1.access.dcui.get	Get information about the state of the Direct Console User Interface (DCUI TTY2).
com.vmware.appliance.version1.access.dcui.set	Set enabled state of the Direct Console User Interface (DCUI TTY2).
com.vmware.appliance.version1.access.shell.get	Get information about the state of Bash shell, that is, access to Bash shell from within the controlled CLI.
com.vmware.appliance.version1.access.shell.set	Set enabled state of Bash shell, that is, access to Bash shell from within the controlled CLI.
com.vmware.appliance.version1.access.ssh.get	Get enabled state of the SSH-based controlled CLI.
com.vmware.appliance.version1.access.ssh.set	Set enabled state of the SSH-based controlled CLI.

API Command	Description
com.vmware.appliance.version1.localaccounts.user.add	Create a new local user account.
com.vmware.appliance.version1.localaccounts.user.delete	Delete a local user account.
com.vmware.appliance.version1.localaccounts.user.get	Get the local user account information.
com.vmware.appliance.version1.localaccounts.user.list	List local user accounts.
com.vmware.appliance.version1.localaccounts.user.password.update	Update the password of a logged in user or of the user that you specify in the username parameter.
com.vmware.appliance.version1.localaccounts.user.set	Update local user account properties, such as role, full name, enabled status, and password.
com.vmware.appliance.version1.monitoring.snmp.disable	Stop an enabled SNMP agent.
com.vmware.appliance.version1.monitoring.snmp.enable	Start a disabled SNMP agent.
com.vmware.appliance.version1.monitoring.snmp.get	Return an SNMP agent configuration.
com.vmware.appliance.version1.monitoring.snmp.hash	Generate localized keys for secure SNMPv3 communications.
com.vmware.appliance.version1.monitoring.snmp.limits	Get SNMP limits information.
com.vmware.appliance.version1.monitoring.snmp.reset	Restore settings to factory defaults.
com.vmware.appliance.version1.monitoring.snmp.set	Set SNMP configuration.
com.vmware.appliance.version1.monitoring.snmp.stats	Generate diagnostics report for SNMP agent.
com.vmware.appliance.version1.networking.dns.domains.add	Add domains to DNS search domains.
com.vmware.appliance.version1.networking.dns.domains.list	Get a list of DNS search domains.
com.vmware.appliance.version1.networking.dns.domains.set	Set DNS search domains.
com.vmware.appliance.version1.networking.dns.hostname.get	Get the Fully Qualified Domain Name.
com.vmware.appliance.version1.networking.dns.hostname.set	Set the Fully Qualified Domain Name.
com.vmware.appliance.version1.networking.dns.servers.add	Add a DNS server. This method fails if you use DHCP.
com.vmware.appliance.version1.networking.dns.servers.get	Get DNS server configuration.
com.vmware.appliance.version1.networking.dns.servers.set	Set the DNS server configuration. If the host is configured to acquire DNS servers and host name by using DHCP, a DHCP refresh is forced.
com.vmware.appliance.version1.networking.firewall.addr.inbound.add	Add a firewall rule to allow or deny access from an incoming IP address.
com.vmware.appliance.version1.networking.firewall.addr.inbound.delete	Delete a specific rule at a given position or delete all rules.
com.vmware.appliance.version1.networking.firewall.addr.inbound.list	Get an ordered list of inbound IP addresses that are allowed or denied by a firewall rule.
com.vmware.appliance.version1.networking.interfaces.get	Get information about a particular network interface.

API Command	Description
com.vmware.appliance.version1.networking.interfaces.list	Get a list of available network interfaces, including interfaces that are not yet configured.
com.vmware.appliance.version1.networking.ipv4.get	Get IPv4 network configuration for interfaces.
com.vmware.appliance.version1.networking.ipv4.list	Get IPv4 network configuration for all configured interfaces.
com.vmware.appliance.version1.networking.ipv4.renew	Renew IPv4 network configuration on interfaces. If the interface is configured to use DHCP for IP address assignment, the lease of the interface is renewed.
com.vmware.appliance.version1.networking.ipv4.set	Set IPv4 network configuration for an interface.
com.vmware.appliance.version1.networking.ipv6.get	Get IPv6 network configuration for interfaces.
com.vmware.appliance.version1.networking.ipv6.list	Get IPv6 network configuration for all configured interfaces.
com.vmware.appliance.version1.networking.ipv6.set	Set IPv6 network configuration for an interface.
com.vmware.appliance.version1.networking.routes.add	Add static routing rules. A destination/prefix of the type 0.0.0.0/0 (for IPv4) or ::/0 (for IPv6) refers to the default gateway.
com.vmware.appliance.version1.networking.routes.delete	Delete static routing rules.
com.vmware.appliance.version1.networking.routes.list	Get routing table. A destination/prefix of the type 0.0.0.0/0 (for IPv4) or ::/0 (for IPv6) refers to the default gateway.
com.vmware.appliance.ntp.get	Get NTP configuration settings. If you run the `tymesync.get` command, you can retrieve the current time synchronization method (by using NTP or VMware Tools). The `ntp.get` command always returns the NTP server information, even when the time synchronization method is not set to NTP. If time synchronization method is not set by using NTP, the NTP status is displayed as down.
com.vmware.appliance.version1.ntp.server.add	Add NTP servers. This command adds NTP servers to the configuration. If the time synchronization is NTP-based, then NTP daemon is restarted to reload the new NTP servers. Otherwise, this command just adds servers to the NTP configuration.

API Command	Description
com.vmware.appliance.version1.ntp.server.delete	Delete NTP servers. This command deletes NTP servers from the configuration. If the time synchronization mode is NTP-based, the NTP daemon is restarted to reload the new NTP configuration. Otherwise, this command just deletes servers from the NTP configuration.
com.vmware.appliance.version1.ntp.server.set	Set NTP servers. This command deletes old NTP servers from the configuration and sets the input NTP servers in the configuration. If the time synchronization is set by using NTP, the NTP daemon is restarted to reload the new NTP configuration. Otherwise, this command just replaces the servers in NTP configuration with the NTP servers that you provide as input.
com.vmware.appliance.version1.resources.cpu.stats.get	Get CPU statistics.
com.vmware.appliance.version1.resources.load.health.get	Get load health.
com.vmware.appliance.version1.resources.load.stats.get	Get load averages (over 1, 5, and 15-minute intervals).
com.vmware.appliance.version1.resources.mem.health.get	Get memory health.
com.vmware.appliance.version1.resources.mem.stats.get	Get memory statistics.
com.vmware.appliance.version1.resources.net.stats.get	Get network statistics.
com.vmware.appliance.version1.resources.net.stats.list	Get network statistics for all interfaces that are up and running.
com.vmware.appliance.version1.resources.processes.stats.list	Get statistics on all processes.
com.vmware.appliance.version1.resources.softwarepackages.health.get	Get the health of the update component.
com.vmware.appliance.version1.resources.storage.health.get	Get storage health statistics.
com.vmware.appliance.version1.resources.storage.stats.list	Get storage statistics for each logical disk.
com.vmware.appliance.version1.resources.swap.health.get	Get swap health.
com.vmware.appliance.version1.resources.swap.stats.get	Get swap statistics.
com.vmware.appliance.version1.resources.system.health.get	Get the overall health of the system.
com.vmware.appliance.version1.resources.system.stats.get	Get the system status.
com.vmware.appliance.version1.services.list	Get the list of all known services.
com.vmware.appliance.version1.services.restart	Restart a service.
com.vmware.appliance.version1.services.status.get	Get the status of a service.
com.vmware.appliance.version1.services.stop	Stop a service.
com.vmware.appliance.version1.system.storage.list	Gets disk to partition mapping.
com.vmware.appliance.version1.system.storage.resize	Resizes all partitions to 100 percent of disk size.

API Command	Description
com.vmware.appliance.version1.system.time.get	Gets system time.
com.vmware.appliance.version1.system.update.get	Get the URL-based patching configuration.
com.vmware.appliance.version1.system.update.set	Set the URL-based patching configuration.
com.vmware.appliance.version1.system.version.get	Get the version of the appliance.
com.vmware.appliance.version1.timesync.get	Get the time synchronization configuration.
com.vmware.appliance.version1.timesync.set	Set the time synchronization configuration.

Configuring SNMP for vCenter Server

vCenter Server includes an SNMP agent that can send trap notifications and receive `GET`, `GETBULK`, and `GETNEXT` requests.

You can use the appliance shell API commands to enable and configure the vCenter Server SNMP agent. You configure the agent differently depending on whether you want to use SNMP v1/v2c or SNMP v3.

SNMP v3 informs are not supported. vCenter Server supports only notifications such as v1 and v2c traps, and v3 traps with all security levels.

Configure the SNMP Agent for Polling

If you configure the vCenter Server SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET`, `GETNEXT`, and `GETBULK` requests.

By default, the embedded SNMP agent listens on UDP port 161 for polling requests from management systems. You can use the `snmp.set --port` command to configure an alternative port. To avoid conflicts between the port for the SNMP agent and the ports of other services, use a UDP port that is not defined in `/etc/services`.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.

   The default user with super administrator role is root.

2. Run the `snmp.set --port` command to configure the port.
   For example, run the following command:

   ```
   snmp.set --port port
   ```

   Here *`port`* is the port for the SNMP agent to use for listening for polling requests.

   Important: The port you specify must not be already in use by other services. Use IP addresses from the dynamic range, port 49152 and up.

3. Optional: If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.

Configure vCenter Serverfor SNMP v1 and v2c

When you configure the vCenter Server SNMP agent for SNMP v1 and v2c, the agent supports sending notifications and receiving `GET` requests.

In SNMP v1 and v2c, community strings are namespaces that contain one or more managed objects. Namespaces can act as a form for authentication, but this does not secure the communication. To secure the communication, use SNMP v3.

Configure SNMP Communities

To enable the vCenter Server SNMP agent to send and receive SNMP v1 and v2c messages, you must configure at least one community for the agent.

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.

   The default user with super administrator role is root.

2. Run the `snmp.set --communities` command to configure an SNMP community.
   For example, to configure public, east, and west network operation center communities, run the following command:

   ```
   snmp.set --communities public,eastnoc,westnoc
   ```

   Each time you specify a community with this command, the settings you specify overwrite the previous configuration.

   To specify multiple communities, separate the community names with a comma.

Configure the SNMP Agent to Send v1 or v2c Notifications

You can use the vCenter ServerSNMP agent to send virtual machine and environmental notifications to management systems.

To send SNMP v1 and v2c notifications with the SNMP agent, you must configure the target, that is the receiver, unicast address, community, and an optional port. If you do not specify a port, the SNMP agent sends notifications to UDP port 162 on the target management system by default.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.

   The default user with super administrator role is root.

2. Run the `snmp.set --targets` command:

   ```
   snmp.set --targets target_address@port/community
   ```

   Here *`target_address`*, *`port`*, and *`community`* are the address of the target system, the port number to send the notifications to, and the community name, respectively. The port value is optional. If you do not specify a port, the default port,161, is used.

   Each time you specify a target with this command, the settings you specify overwrite all previously specified settings. To specify multiple targets, separate them with a comma.

   For example, run the following command for configuring the targets 192.0.2.1@678/targetcommunity and 2001:db8::1/anothercom:

   ```
   snmp.set --targets 192.0.2.1@678/targetcommunity,2001:db8::1/anothercom
   ```

3. Optional: If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.

4. Optional: To send a test trap to verify that the agent is configured correctly, run the `snmp.test` command.

   The agent sends a `warmStart` trap to the configured target.

Configure vCenter Server for SNMP v3

When you configure the SNMP agent for SNMP v3, the agent supports sending traps. SNMP v3 also provides stronger security than v1 or v2c, including cryptographic authentication and encryption.

SNMP v3 informs are not supported. vCenter Server supports only notifications such as v1/v2c traps and v3 traps with all security levels.

Configure the SNMP Engine ID

Every SNMP v3 agent has an engine ID, which serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate localized keys for authentication and encryption of SNMP v3 messages.

If you do not specify an engine ID before you enable the SNMP agent, when you enable the standalone SNMP agent, an engine ID is generated.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Run the `snmp.set --engineid` command to configure the target.
   For example, run the following command:
   ```
   snmp.set --engineid 80001adc802417e202b8613f5400000000
   ```
   Here, 80001adc802417e202b8613f5400000000 is the ID, a hexadecimal string between 5 and 32 characters in length.

Configure SNMP Authentication and Privacy Protocols

SNMP v3 optionally supports authentication and privacy protocols.

Authentication is used to ensure the identity of users. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data. The privacy protocols provide a higher level of security than is available in SNMP v1 and v2c, which use community strings for security.

Both authentication and privacy are optional. However, you must enable authentication if you plan to enable privacy.

The SNMP v3 authentication and privacy protocols are licensed vSphere features and might not be available in some vSphere editions.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Optional: Run the `snmp.set --authentication` command to configure authentication.
   For example, run the following command:
   ```
   snmp.set --authentication protocol
   ```
   Here, *`protocol`* must be either `none`, for no authentication,`SHA1`, or `MD5`.
3. Optional: Run the `snmp.set --privacy` command to configure privacy protocol.
   For example, run the following command:
   ```
   snmp.set --privacy protocol
   ```
   Here, *`protocol`* must be either `none`, for no privacy, or `AES128`.

Configure SNMP Users

You can configure up to five users who can access SNMP v3 information. User names must be no more than 32 characters long.

- Verify that you have configured the authentication and privacy protocols before configuring users.
- Verify that you know the authentication and privacy passwords for each user that you plan to configure. Passwords must be at least eight characters long. Store these passwords in files on the host system.

While configuring a user, you generate authentication and privacy hash values based on the user's authentication and privacy passwords and on the SNMP agent's engine ID. After configuring users, if you change the engine ID, the authentication protocol, or the privacy protocol, the users are no longer valid and must be reconfigured.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.

2. If you are using authentication or privacy, get the authentication and privacy hash values for the user by the running `snmp.hash --auth_hash --priv_hash` command.
   For example, run the following command:
   ```
   snmp.hash  --auth_hash secret1 --priv_hash secret2
   ```
   Here, *secret1* is the path to the file containing the user's authentication password and *secret2* is the path to the file containing the user's privacy password. Alternatively, you can specify the flag `--raw_secret` and set the boolean parameter to *true*.

   The authentication and privacy hash values are displayed.

3. Configure the user by running `snmp.set --user`.
   For example, run the following command:
   ```
   snmp.set --user userid/authhash/privhash/security
   ```
   The parameters in the command are as follows.

Parameter	Description
userid	Replace with the user name.
authhash	Replace with the authentication hash value.
privhash	Replace with the privacy hash value.
security	Replace with the level of security enabled for that user, which can be `auth`, for authentication only, `priv`, for authentication and privacy, or `none`, for no authentication or privacy.

Configure SNMP v3 Targets

Configure SNMP v3 targets to allow the SNMP agent to send SNMP v3 traps.

You can configure a maximum of three SNMP v3 targets, in addition to a maximum of three SNMP v1 or v2c targets.

To configure a target, you must specify a host name or IP address of the system that receives the traps, a user name, a security level, and whether to send traps. The security level can be either `none`, for no security, `auth`, for authentication only, or `priv`, for authentication and privacy.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Run the `snmp.set --v3targets` command to set up the SNMP v3 target.
   For example, run the following command:
   ```
   snmp.set --v3targets hostname@port/userid/secLevel/trap
   ```
   The parameters in the command are as follows.

Parameter	Description
hostname	Replace with the host name or IP address of the management system that receives the traps.
port	Replace with the port on the management system that receives the traps. If you do not specify a port, the default port, 161, is used.
userid	Replace with the user name.

Parameter	Description
secLevel	Replace with either `none`, `auth`, or `priv` to indicate the level of authentication and privacy you have configured. Use `auth` if you have configured authentication only, `priv` if you have configured both authentication and privacy, and `none` if you have configured neither.

3. Optional: If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.
4. Optional: To send a test trap to verify that the agent is configured correctly, run the `snmp.test` command.
   The agent sends a `warmStart` trap to the configured target.

Configure the SNMP Agent to Filter Notifications

You can configure the vCenter Server SNMP agent to filter out notifications if you do not want your SNMP management software to receive those notifications.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Run the `snmp.set --notraps` command to filter traps.
   - To filter specific traps, run the following command:
     `snmp.set --notraps` *`oid_list`*
     Here, *`oid_list`* is a list of object IDs for the traps to filter, separated by commas. This list replaces any object IDs that were previously specified using this command.
   - To clear all trap filters, run the following command:
     `snmp.set --notraps reset`
3. Optional: If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.

The traps identified by the specified object IDs are filtered out of the output of the SNMP agent, and are not sent to SNMP management software.

Configure SNMP Management Client Software

After you have configured vCenter Server to send traps, you must configure your management client software to receive and interpret those traps.

Download the VMware MIB files from https://kb.vmware.com/s/article/1013445.

To configure your management client software, specify the communities for the managed device, configure the port settings, and load the VMware MIB files. See the documentation for your management system for specific instructions for these steps.

1. In your management software, specify the vCenter Server instance as an SNMP-based managed device.
2. If you are using SNMP v1 or v2c, set up appropriate community names in the management software.
   These names must correspond to the communities set for the SNMP agent on vCenter Server.

3. If you are using SNMP v3, configure users and authentication and privacy protocols to match the protocols configured on vCenter Server.
4. If you configured the SNMP agent to send traps to a port on the management system other than the default UDP port 162, configure the management client software to listen on the port you configured.
5. Load the VMware MIBs into the management software to view the symbolic names for the vCenter Server variables.

   To prevent lookup errors, load these MIB files in the following order before loading other MIB files:

   1. `VMWARE-ROOT-MIB.mib`
   2. `VMWARE-TC-MIB.mib`
   3. `VMWARE-PRODUCTS-MIB.mib`

The management software can now receive and interpret traps from vCenter Server.

Reset SNMP Settings to Factory Defaults

You can reset SNMP settings to factory defaults. You can also reset the value of a specific argument to the factory default.

You can reset a specific argument, such as the communities or targets. You can also reset the SNMP configuration to the factory defaults.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.

   The default user with super administrator role is root.
2. To reset specific arguments, run the command `snmp.set --arguments reset`.
   For example, to reset the communities that you configured, run the following command:

   ```
   snmp.set --communities reset
   ```
3. To reset the whole SNMP configuration to the factory defaults, run the command `snmp.reset`.

Configuring Time Synchronization Settings in vCenter Server

You can change the time synchronization settings in vCenter Server after deployment.

When you deploy vCenter Server, you can choose the time synchronization method to be either by using an NTP server or by using VMware Tools. In case the time settings in your vSphere network change, you can edit the vCenter Server and configure the time synchronization settings by using the commands in the appliance shell.

When you enable periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host.

After time synchronization occurs, VMware Tools checks once every minute to determine whether the clocks on the guest operating system and the host still match. If not, the clock on the guest operating system is synchronized to match the clock on the host.

Native time synchronization software, such as Network Time Protocol (NTP), is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred. You can use only one form of periodic time synchronization in vCenter Server. If you decide to use native time synchronization software, vCenter Server VMware Tools periodic time synchronization is disabled, and the reverse.

Related Links

Synchronize ESXi Clocks with a Network Time Server on page 1373

Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

Use VMware Tools Time Synchronization

You can set up vCenter Server to use VMware Tools time synchronization.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Run the command to enable VMware Tools time synchronization.
   ```
   timesync.set --mode host
   ```
3. Optional: Run the command to verify that you successfully applied the VMware Tools time synchronization.
   ```
   timesync.get
   ```
   The command returns that the time synchronization is in host mode.

The time of the appliance is synchronized with the time of the ESXi host.

Add or Replace NTP Servers in the vCenter Server Configuration

To set up the vCenter Server to use NTP-based time synchronization, you must add the NTP servers to the vCenter Server configuration.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Add NTP servers to the vCenter Server configuration by running the following `ntp.set` command.
   ```
   ntp.set --servers IP-addresses-or-host-names
   ```
   In this command, *`IP-addresses-or-host-names`* is a comma-separated list of IP addresses or host names of the NTP servers.
   This command removes the current NTP servers (if any) and adds the new NTP servers to the configuration. If the time synchronization is based on an NTP server, then the NTP daemon is restarted to reload the new NTP servers. Otherwise, this command replaces the current NTP servers in the NTP configuration with the new NTP servers you specify.
3. Optional: To verify that you successfully applied the new NTP configuration settings, run the following command.
   ```
   ntp.get
   ```
   The command returns a space-separated list of the servers configured for NTP synchronization. If the NTP synchronization is enabled, the command returns that the NTP configuration is in Up status. If the NTP synchronization is disabled, the command returns that the NTP configuration is in Down status.
4. Optional: To verify if the NTP server is reachable, run the following command.
   ```
   ntp.test --servers IP-addresses-or-host-names
   ```
   The command returns the status of the NTP servers.

If the NTP synchronization is disabled, you can configure the time synchronization settings in the vCenter Server to be based on an NTP server. See Synchronize the Time in vCenter Server with an NTP Server.

Synchronize the Time in vCenter Server with an NTP Server

You can configure the time synchronization settings in the vCenter Server to be based on an NTP server.

Set up one or more Network Time Protocol (NTP) servers in the vCenter Server configuration. See Add or Replace NTP Servers in the vCenter Server Configuration.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.

2. Run the command to enable NTP-based time synchronization.
   ```
   timesync.set --mode NTP
   ```
3. Optional: Run the command to verify that you successfully applied the NTP synchronization.
   ```
   timesync.get
   ```
   The command returns that the time synchronization is in NTP mode.

Managing Local User Accounts in vCenter Server

If you log in to the appliance shell as a super administrator, you can manage the local user accounts in vCenter Server by running commands in the appliance shell. The default user with a super administrator role is root.

User Roles in vCenter Server

There are three main user roles in vCenter Server.

The local users of vCenter Server have the rights to perform various tasks. Three user roles are available in vCenter Server:

Operator	Local users with the operator user role can read vCenter Server configuration.
Administrator	Local users with the administrator user role can configure vCenter Server.
Super Administrator	Local users with the super administrator user role can configure vCenter Server, manage the local accounts, and use the Bash shell.

Get a List of the Local User Accounts in vCenter Server

You can see the list of the local user accounts so that you can decide which user account to manage from the appliance shell.

1. Access the appliance shell and log in as a user who has a super administrator role.
   The default user with a super administrator role is root.
2. Run the `localaccounts.user.list` command.
   You can see a list of the local users. The information about a user includes the user name, status, role, status of the password, full name, and email.

   Note: The list of local users includes only the local users who have their default shell as appliance shell.

Create a Local User Account in vCenter Server

You can create a new local user account.

For information about the user roles, see User Roles in vCenter Server.

1. Access the appliance shell and log in as a user who has a super administrator role.
   The default user with a super administrator role is root.

2. Run the `localaccounts.user.add --role --username --password` command.
   For example, to add the local user account test with the operator user role, run the following command:
   ```
   localaccounts.user.add --role operator --username test --password
   ```
   The role can be `operator`, `admin`, or `superAdmin`.
   You can also set up a new local user account and specify an email and the full name of the user. For example, to add the local user account test1 with the operator user role, full name TestName and the email address test1@mymail.com, run the following command:
   ```
   localaccounts.user.add --role operator --username test1 --password --fullname TestName --email test1@mymail.com
   ```
   You cannot use spaces in full names.
3. Enter and confirm the password of the new local user when prompted.

You created a new local user in the appliance.

Update the Password of a Local User in vCenter Server

You can update the password of a local user in vCenter Server for security reasons.

1. Access the appliance shell and log in as a user who has a super administrator role.
   The default user with a super administrator role is root.
2. Run the `localaccounts.user.password.update --username user name --password` command.
   For example, to change the password of a user with user name test, run the following command:
   ```
   localaccounts.user.password.update --username test --password
   ```
3. Enter and confirm the new password when prompted.

Update a Local User Account in vCenter Server

You can update an existing local user account in vCenter Server.

For information about the user roles, see User Roles in vCenter Server.

1. Access the appliance shell and log in as a user who has a super administrator role.
   The default user with a super administrator role is root.
2. Run the `localaccounts.user.set --username` command to update an existing local user.
   - To update the role of the local user, run the following command:
     ```
     localaccounts.user.set --username user name --role new role
     ```
     Here, *`user name`* is the name of the user that you want to edit and *`new role`* is the new role. The role can be `operator`, `admin`, or `superAdmin`.
   - To update the email of the local user, run the following command:
     ```
     localaccounts.user.set --username user name --email new email address
     ```
     Here, *`user name`* is the name of the user that you want to edit and *`new email address`* is the new email address.
   - To update the full name of the local user, run the following command:
     ```
     localaccounts.user.set --username user name --fullname new full name
     ```
     Here, *`user name`* is the name of the user that you want to edit and *`new full name`* is the new full name of the user.
   - To update the status of the local user, run the following command:
     ```
     localaccounts.user.set --username user name --status new status
     ```
     Here, *`user name`* is the name of the user that you want to edit and *`status`* is the new status of the local user. The status can be either `disabled` or `enabled`.

Delete a Local User Account in vCenter Server

You can delete a local user account in vCenter Server.

1. Access the appliance shell and log in as a user who has a super administrator role.
   The default user with a super administrator role is root.
2. Run the `localaccounts.user.delete --username` command.
   For example, to delete the user with user name test, run the following command:
   ```
   localaccounts.user.delete --username test
   ```
   The user is deleted.

Monitor Health Status and Statistics in vCenter Server

You can monitor the hardware health status of vCenter Server by using the API commands in the appliance shell. You can also monitor the health status of the update component for information about available patches.

You can view the status of the hardware components such as memory, CPU, storage, and network, as well as the update component that shows if the software packages are up to date according to the last check for available patches.
A particular health status can be green, yellow, orange, red, or gray. For more information, see View vCenter ServerHealth Status.

For a complete list of the API commands that you can use for monitoring statistics and health of the vCenter Server system, see API Commands in the Appliance Shell.

1. Access the appliance shell and log in.
   The user name that you use to log in can be of a user with an operator, administrator, or super administrator user role.
2. View the health status of a particular component.
   - To view the health of the memory in vCenter Server, run the `mem.health.get` command.
   - To view the health of the storage in vCenter Server, run the `storage.health.get` command.
   - To view the health of the swap in vCenter Server, run the `swap.health.get` command.
   - To view the health of the update component in vCenter Server, run the `softwarepackages.health.get` command.

     Important: If you do not perform regular checks for available patches, the health status of the update component might become out-of-date. For information about checking for vCenter Server patches and enabling automatic checks for vCenter Server patches, see *vSphere Upgrade*.
   - To view the overall health of the vCenter Server system, run the `health.system.get` command.
3. To view statistics about a particular hardware component, run the respective command.
   For example, to view storage statistics for each logical disk, run the `storage.stats.list` command.

Using the vimtop Plug-In to Monitor the Resource Use of Services

You can use the `vimtop` utility plug-in to monitor vSphere services that run in the vCenter Server.

`vimtop` is a tool similar to `esxtop`, which runs in the environment of the vCenter Server. By using the text-based interface of `vimtop` in the appliance shell, you can view overall information about the vCenter Server, and a list of vSphere services and their resource use.

Monitor Services By Using vimtop in Interactive Mode

You can use the `vimtop` plug-in to monitor services in real time.

The default view of the `vimtop` interactive mode consists of the overview tables and the main table. You can use single-key commands in interactive mode to switch the view from processes to disks or network.

1. From an SSH client application, log in to the vCenter Server shell.
2. Run the `vimtop` command to access the plug-in in interactive mode.

Related Links

Interactive Mode Command-Line Options on page 1727
You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Interactive Mode Single-Key Commands for vimtop on page 1727
When running in interactive mode, `vimtop` recognizes several single-key commands.

Interactive Mode Command-Line Options

You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Table 135: Interactive Mode Command-Line Options

Option	Description
-h	Prints help for the `vimtop` command-line options.
-v	Prints the `vimtop` version number.
-c *filename*	Loads a user-defined `vimtop` configuration file. If the -c option is not used, the default configuration file is `/root/vimtop/vimtop.xml`. You can create your own configuration file, specifying a different filename and path by using the `W` single-key interactive command.
-n *number*	Sets the number of performed iterations before the `vimtop` exits interactive mode. `vimtop` updates the display *number* number of times and exits. The default value is 10000.
-p / -d*seconds*	Sets the update period in seconds.

Related Links

Monitor Services By Using vimtop in Interactive Mode on page 1727
You can use the `vimtop` plug-in to monitor services in real time.

Interactive Mode Single-Key Commands for vimtop on page 1727
When running in interactive mode, `vimtop` recognizes several single-key commands.

Interactive Mode Single-Key Commands for vimtop

When running in interactive mode, `vimtop` recognizes several single-key commands.

All interactive mode panels recognize the commands listed in the following table.

Table 136: Interactive Mode Single-Key Commands

Key Names	Description
h	Show a help menu for the current panel, giving a brief summary of commands, and the status of secure mode.
i	Show or hide the top line view of the overview panel of the `vimtop` plug-in.
t	Show or hide the Tasks section, which displays information in the overview panel about the tasks currently running on the vCenter Server instance.
m	Show or hide the Memory section in the overview panel.
f	Show or hide the CPU section which displays information in the overview panel about all available CPUs.
g	Show or hide the CPUs section which displays information in the overview panel about the top 4 physical CPUs.
spacebar	Immediately refreshes the current pane.
p	Pause the displayed information about the services resource use in the current panels.
r	Refresh the displayed information about the services resource use in the current panels.
s	Set refresh period.
q	Exit the interactive mode of the `vimtop` plug-in.
k	Displays the Disks view of the main panel.
o	Switch the main panel to Network view.
Esc	Clear selection or return to the Processes view of the main panel.
Enter	Select a service to view additional details.
n	Show or hide names of the headers in the main panel.
u	Show or hide the measurement units in the headers in the main panel.
left, right arrows	Select columns.
up, down arrows	Select rows.
<,>	Move a selected column.
Delete	Remove selected column.
c	Add a column to the current view of the main panel. Use spacebar to add or remove columns from the displayed list.
a	Sort the selected column in ascending order.
d	Sort the selected column in descending order.
z	Clear the sort order for all columns.
l	Set width for the selected column.
x	Return the column widths to their default values.
+	Expand selected item.
-	Collapse selected item.
w	Write the current setup to a `vimtop` configuration file. The default file name is the one specified by -c option, or `/root/vimtop/vimtop.xml` if the -c option is not used. You can also specify a different file name on the prompt generated by the `w` command.

Related Links

Monitor Services By Using vimtop in Interactive Mode on page 1727
You can use the `vimtop` plug-in to monitor services in real time.

Interactive Mode Command-Line Options on page 1727
You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Using the Direct Console User Interface to Configure vCenter Server

After you deploy vCenter Server, you can reconfigure the network settings and enable access to the Bash shell for troubleshooting. To access the Direct Console User Interface, you must log in as root.

The home page of the Direct Console User Interface contains a link to the support bundle of the vCenter Server. The link to the support bundle is of the type https://*appliance-host-name*:443/appliance/support-bundle.

Log In to the Direct Console User Interface

The Direct Console User Interface lets you interact with vCenter Server locally by using text-based menus.

1. From the vSphere Client, navigate to the host and click **Configure** > **Services**. Confirm that the SSH and Direct Console User Interface services are running.
2. Open an SSH client and connect to the ESXi host.
3. Log in with the root account.
4. Enter `DCUI` to start the Direct Console User Interface.
5. Click inside the console window and press F2 to customize the system.
6. Type the password for the root user and press Enter.

   Important: If you enter invalid credentials thrice, the root account is locked for five minutes.

You logged in to the Direct Console User Interface. You can change the password of the root user, edit the network settings, and enable access to the vCenter Server appliance Bash shell.

Change the Password of the Root User

To prevent unauthorized access to the vCenter Server Direct Console User Interface, you can change the password of the root user.

The default root password for the vCenter Server instance is the password you enter during deployment.

Important: The password for the root account of vCenter Server expires after 90 days. You can change the expiry time for an account by logging as root to the vCenter Server Bash shell, and running `chage -M number_of_days -W warning_until_expirationuser_name`. To increase the expiration time of the root password to infinity, run the `chage -M -1 -E -1 root` command.

1. Log in to the Direct Console User Interface.
2. Select **Configure Password** and press Enter.
3. Type the old password of the root user, and press Enter.
4. Set up the new password and press Enter.
5. Press Esc until you return to the main menu of the Direct Console User Interface.

You changed the password of the root user of the appliance.

Configure the Management Network of vCenter Server

The vCenter Server instance can obtain networking settings from a DHCP server, or use static IP addresses. You can change the networking settings of vCenter Serverfrom the Direct Console User Interface. You can change the IPv4, IPv6, and DNS configuration.

To change the IP address of the vCenter Server instance, verify that the system name is an FQDN. If, during deployment you set an IP address as a system name, you cannot change the IP address after the deployment. The system name is always used as a primary network identifier.

1. Log in to the Direct Console User Interface of vCenter Server
2. Select **Configure Management Network** and press Enter.
3. Change the IPv4 settings from **IP Configuration**.

Option	Description
Use dynamic IP address and network configuration	Obtains networking settings from a DHCP server if one is available on your network
Set static IP address and network configuration	Sets static networking configuration

4. Change the IPv6 settings from **IPv6 Configuration**.

Option	Description
Enable IPv6	Enables or disables IPv6
Use DHCP stateful configuration	Uses a DHCP server to obtain IPv6 addresses and networking settings
Use ICMP stateless configuration	Uses a Stateless Address Autoconfiguration (SLAAC) to obtain IPv6 addresses and network settings

5. Change the DNS settings from **DNS Configuration**.

Option	Description
Obtain DNS server address and hostname automatically	Obtains the DNS server address and host name automatically. Use this option if the IP settings are obtained automatically from a DHCP server.
Use the following DNS server address and hostname	Sets the static IP address and host name for the DNS server.

6. Set custom DNS suffixes from **Custom DNS Suffixes**.

   If you do not specify any suffixes, a default suffix list is derived from the local domain name.

7. Press Esc until you return to the main menu of the Direct Console User Interface.

Restart the Management Network of vCenter Server

Restart the management network of vCenter Server to restore the network connection.

1. Log in to the Direct Console User Interface of vCenter Server.
2. Select **Restart Management Network** and press Enter.
3. Press F11.

Enable Access to the Bash Shell

You can use the Direct Console User Interface to enable local and remote access to the Bash shell. Bash shell access enabled through Direct Console User Interface remains enabled for 3600 seconds.

1. Log in to the Direct Console User Interface of vCenter Server.
2. Select **Troubleshooting Options** and press Enter.
3. From the Troubleshooting Mode Options menu, select to enable either Bash shell or SSH.
4. Press Enter to enable the service.
5. Press Esc until you return to the main menu of the Direct Console User Interface.

Access the vCenter Server Bash shell for troubleshooting.

Access the Bash Shell for Troubleshooting

Log in to the Bash shell for troubleshooting purposes only.

1. Access the shell using one of the following methods.
   - If you have direct access to the vCenter Server instance, press Alt+F1.
   - If you want to connect remotely, use SSH or another remote console connection to start a session.
2. Enter a user name and password.
3. In the shell, enter the command `pi shell` or `shell` to access the Bash shell.

Export a vCenter Server Support Bundle for Troubleshooting

You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

You can also collect the support bundle from the vCenter Server appliance Bash shell by running the `vc-support.sh` script.

The support bundle is exported in `.tgz` format.

1. Log in to the Windows host machine on which you want to download the bundle.
2. Open a Web browser and enter the URL to the support bundle displayed in the DCUI.
   https://*`appliance-fully-qualified-domain-name`*:443/appliance/support-bundle
3. Enter the user name and password of the root user.
4. Click **Enter**.

   The support bundle is downloaded as `.tgz` file on your Windows machine.

Related Links

Retrieve Installation Logs Manually on page 1297

You can retrieve the installation log files manually for examination.

Collect Deployment Log Files for the vCenter Server Appliance on page 1298

If the vCenter Server appliance deployment fails, you can retrieve the log files and examine them for the reason of the failure.

vCenter Server and Host Management

Learn how to use the VMware®vSphere Client components, configure and manage hosts, migrate virtual machines, and manage licenses in your vCenter Server environment.

vCenter Server and Host Management also provides brief introductions to the various tasks you can perform within the system, and it cross-references to the documentation that describes the tasks in detail.

vCenter Server and Host Management covers ESXi and vCenter Server.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

vCenter Server and Host Management is intended for system administrators who are experienced Windows or Linux system administrators and who are familiar with virtual machine technology and data center operations.

Updated Information

This *vCenter Server and Host Management* guide is updated with each release of the product or when necessary.

This table provides the update history of the *vCenter Server and Host Management* guide.

Revision	Description
30 APR 2024	Updated the information about selecting the destination storage for the virtual machine migration in Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion and Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion.
08 JAN 2024	• Added a note about naming inventory objects in Organizing Your Inventory. • Minor change in Limits on Simultaneous Migrations. • Minor change in Disconnecting and Reconnecting an ESXi Host.
20 SEP 2023	Updated the list of supported browser versions in Using the vSphere Client.
01 SEP 2023	• Updated the list of best practices in vSphere Tagging Best Practices. • Added links in Host Configuration for vMotion. • Added information about required ports and ESXi host version in Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion. • Added information about required ports and ESXi host version in Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion. • Added a note related to overriding the default gateway in Place vMotion Traffic on the vMotion TCP/IP Stack of an Host.
17 MAY 2023	Minor update to How to Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.
17 MAR 2023	• Updated the prerequisites in Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion.

Revision	Description
	• Updated the prerequisites in Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion.
17 FEB 2023	• Added a note about networking settings in Use Quickstart to Extend a Cluster with Host Networking Configuration. • Added a note about networking settings in Add a Host to a Cluster.
10 JAN 2023	Updated the steps in Export Lists.
21 NOV 2022	• Added a new topic, How Do You Cancel a vSphere Task. • Updated the steps in Sort the vSphere Client Inventory. • Updated the requirement for migrating a virtual machine with NVIDIA vGPU in Migrate a Virtual Machine to New Storage. • Minor updates to Reboot or Shut Down an ESXi Host and vSphere Tagging Best Practices.
7 OCT 2022	Updated the vSphere+ and vSAN+ Subscriptions topic.
12 JULY 2022	• Added information about vSphere+ and vSAN+. See License and Subscription Management. • Updated the licensing requirements for migrating virtual machines. See Requirements for vMotion Between vCenter Server Instances.
10 JUNE 2022	Added the Configure the vSphere Client Timeout Value procedure.
10 MAY 2022	Added information about the estimated worst-case stun times. See Using vMotion to Migrate vGPU Virtual Machines.
5 MAY 2022	Updated the Change the EVC Mode for a Cluster procedure.
24 JAN 2022	Updated the Export Lists procedure.
14 DEC 2021	Minor update to Encrypted vSphere vMotion.
05 OCT 2021	Initial release.

vSphere Concepts and Features

VMware vSphere® uses the power of virtualization to transform data centers into simplified cloud computing infrastructures, enabling IT organizations to deliver flexible and reliable IT services.

The two core components of vSphere are VMware ESXi™ and VMware vCenter Server®. ESXi is the hypervisor on which you create and run virtual machines. vCenter Server is a service that acts as a central administrator for ESXi hosts that are connected on a network. With vCenter Server, you can pool and manage the resources of multiple hosts. vCenter Server allows you to monitor and manage your physical and virtual infrastructure.

Additional vSphere components are available as plugins that extend the functionality of the vSphere product.

Virtualization Basics

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The hypervisor serves as a platform for running virtual machines and allows for the consolidation of computing resources.

Each virtual machine contains its own virtual, or software-based, hardware, including a virtual CPU, memory, hard disk, and network interface card.

ESXi is the hypervisor in a vSphere environment. The hypervisor is installed on physical or virtual hardware in a virtualized data center, and acts as a platform for virtual machines. The hypervisor provides physical hardware resources dynamically to virtual machines to support the operation of the virtual machines. The hypervisor allows virtual machines to operate with a degree of independence from the underlying physical hardware. For example, a virtual machine can be

moved from one physical host to another, or its virtual disks can be moved from one type of storage to another, without affecting the functioning of the virtual machine.

Because virtual machines are decoupled from the underlying physical hardware, virtualization allows you to consolidate physical computing resources such as CPUs, memory, storage, and networking into pools of resources. These resources can be dynamically and flexibly made available to virtual machines. With the vCenter Server management platform, you can increase the availability and security of your virtual infrastructure.

Physical Topology of vSphere Data Center

A typical VMware vSphere data center consists of physical building blocks such as x86 virtualization servers, storage networks and arrays, IP networks, a management server, and desktop clients.

The vSphere data center includes the following components.

ESXi Hosts	Industry standard x86 servers that run ESXi on the bare metal. ESXi software provides resources for and runs the virtual machines. You can group a number of similarly configured x86 servers with connections to the same network and storage subsystems. This grouping creates an aggregate set of resources in the virtual environment, called a cluster.
Storage networks and arrays	VMware vSphere uses Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays to meet different data center storage needs. With storage area networks, you can connect and share storage arrays between groups of servers. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines. For detailed information, see *vSphere Storage*.
IP networks	Each compute server can have multiple physical network adapters to provide high bandwidth and reliable networking to the entire VMware vSphere data center. For detailed information, see *vSphere Networking*.
vCenter Server	vCenter Server provides a single point of control to the data center. It provides essential data center services such as access control, performance monitoring, and configuration. It unifies the resources from the individual computing servers to be shared among virtual machines in the entire data center. It manages the assignment of virtual machines to the ESXi hosts and the assignment of resources to the virtual machines within a given computing server. These assignments are based on the policies that the system administrator sets. Compute servers continue to function even if vCenter Server becomes unreachable (for example, if the network is severed). The ESXi hosts can be managed separately and continue to run the virtual machines assigned to them based on the resource assignment that was last set. After connection to vCenter Server is restored, it can manage the data center as a whole again.
Management clients	VMware vSphere provides several interfaces for data center management and virtual machine access. These interfaces include vSphere Client for access through a web browser or vSphere Command-Line Interface (vSphere CLI).

vSphere Software Components

VMware vSphere is a suite of software components for virtualization. These include ESXi, vCenter Server, and other software components that fulfill several different functions in the vSphere environment.

vSphere includes the following software components:

ESXi

The hypervisor runs virtual machines. Each virtual machine has a set of configuration and disk files that together perform all the functions of a physical machine.

Through ESXi, you run the virtual machines, install operating systems, run applications, and configure the virtual machines. Configuration includes identifying the virtual machine's resources, such as storage devices.

The server provides bootstrapping, management, and other services that manage your virtual machines.

vCenter Server

A service that acts as a central administrator for VMware ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the ESXi hosts.

vCenter Server is installed to run automatically on a preconfigured virtual machine. The vCenter Server service runs continuously in the background. It performs its monitoring and managing activities even when no vSphere Clients are connected and when no one is logged on to the computer where it resides. It must have network access to all the hosts it manages.

vCenter Server is deployed as a preconfigured virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy vCenter Server on ESXi hosts 6.5 or later.

All prerequisite services for running vCenter Server and the vCenter Server components are bundled in the vCenter Server installation. All vCenter Server services run as child processes of the VMware Service Library Lifecycle Manager service. See the *vCenter Server Installation and Setup* documentation for details about setting up this configuration.

vCenter Single Sign-On

A service that is part of the vCenter Server management infrastructure. The vCenter Single Sign-On authentication service makes the VMware cloud infrastructure platform more secure by allowing the various vSphere software components to communicate with each other. The vCenter Single Sign-On authentication service uses a secure token exchange mechanism instead of requiring each component to authenticate a user separately with a directory service like Active Directory.

When you install vCenter Single Sign-On, the following components are deployed.

STS (Security Token Service)	STS certificates enable a user who has logged on through vCenter Single Sign-On to authenticate to any vCenter service that vCenter Single Sign-On supports. The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in each of the vCenter Single Sign-On identity sources.
Administration server	The administration server allows users with vCenter

		Single Sign-On administrator privileges to configure the vCenter Single Sign-On service and manage users and groups from the vSphere Client. Initially, only the user administrator@vsphere.local has these privileges.
	vCenter Lookup Service	vCenter Lookup Service contains topology information about the vSphere infrastructure, enabling vSphere components to connect to each other securely. Unless you are using Simple Install, you are prompted for the Lookup Service URL when you install other vSphere components. For example, the Inventory Service and the vCenter Server installers ask for the Lookup Service URL and then contact the Lookup Service to find vCenter Single Sign-On. After installation, the Inventory Service and vCenter Server system are registered with the vCenter Lookup Service so other vSphere components, like the vSphere Client, can find them.
	VMware Directory Service	Directory service associated with the vsphere.local domain. This service is a multi-tenanted, peer-replicating directory service that makes an LDAP directory available on port 389. In multisite mode, an update of VMware Directory Service content in one VMware Directory Service instance results in the automatic update of the VMware Directory Service instances associated with all other vCenter Single Sign-On nodes.
vCenter Server plug-ins	Applications that provide additional features and functionality to vCenter Server. Typically, plug-ins consist of a server component and a client component. After the plug-in server is installed, it is registered with vCenter Server and the plug-in client is available to the for download. After a plug-in is installed on the vSphere Client, it might alter the interface by adding views, tabs, toolbar buttons, or menu items related to the added functionality. Plug-ins leverage core vCenter Server capabilities, such as authentication and permission management, but can have their own types of events, tasks, metadata, and privileges.	

	Some vCenter Server features are implemented as plug-ins, and can be managed using the vSphere Client Plug-in Manager. These features include vCenter Storage Monitoring, vCenter Hardware Status, and vCenter Service Status.
vCenter Server database	Persistent storage for maintaining the status of each virtual machine, host, and user managed in the vCenter Server environment. The vCenter Server database can be remote or local to the vCenter Server system. The database is installed and configured during vCenter Server installation. If you are accessing your ESXi host directly through the VMware Host Client, and not through a vCenter Server system and associated , you do not use a vCenter Server database.
tcServer	Many vCenter Server functions are implemented as web services that require the tcServer. The tcServer is installed on the vCenter Server machine as part of the vCenter Server installation. Features that require the tcServer to be running include: ICIM/ Hardware Status tab, Performance charts, WebAccess, Storage Policy-Based services, and vCenter Service status.
vCenter Server agent	On each managed host, the software that collects, communicates, and runs the actions received from vCenter Server. The vCenter Server agent is installed the first time any host is added to the vCenter Server inventory.
Host agent	On each managed host, the software that collects, communicates, and runs the actions received through the vSphere Client. It is installed as part of the ESXi installation.

vSphere Cluster Services

vSphere Cluster Services (vCLS) is activated by default and runs in all vSphere clusters. vCLS ensures that if vCenter Server becomes unavailable, cluster services remain available to maintain the resources and health of the workloads that run in the clusters. vCenter Server is still required to run DRS and HA.

vCLS is activated when you upgrade to vSphere 7.0 Update 3 or when you have a new vSphere 7.0 Update 3 deployment. vCLS is upgraded as part of vCenter Server upgrade.

vCLS uses agent virtual machines to maintain cluster services health. The vCLS agent virtual machines (vCLS VMs) are created when you add hosts to clusters. Up to three vCLS VMs are required to run in each vSphere cluster, distributed within a cluster. vCLS is also activated on clusters which contain only one or two hosts. In these clusters the number of vCLS VMs is one and two, respectively.

New anti-affinity rules are applied automatically. Every three minutes a check is performed, if multiple vCLS VMs are located on a single host they will be automatically redistributed to different hosts.

Table 137: Number of vCLS Agent VMs in Clusters

Number of Hosts in a Cluster	Number of vCLS Agent VMs
1	1
2	2
3 or more	3

vCLS VMs run in every cluster even if cluster services like vSphere DRS or vSphere HA are not activated on the cluster. The life cycle operations of vCLS VMs are managed by vCenter Server services like ESX Agent Manager and Workload Control Plane. vCLS VMs do not support NICs.

A cluster activated with vCLS can contain ESXi hosts of different versions if the ESXi versions are compatible with vCenter Server. vCLS works with vSphere Lifecycle Manager clusters.

vSphere DRS

vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere cluster. DRS depends on the availability of vCLS VMs.

Note: If you try to activate DRS on a cluster where there are issues with the vCLS VMs, a warning message is displayed on the **Cluster Summary** page.

Note: If DRS is on but there are issues with the vCLS VMs, you must resolve these issues for DRS to operate. A warning message is displayed on the **Cluster Summary** page.

If DRS is non-functional this does not mean that DRS is deactivated. Existing DRS settings and resource pools survive across a lost vCLS VMs quorum. vCLS health turns **Unhealthy** only in a DRS activated cluster when vCLS VMs are not running and the first instance of DRS is skipped because of this. vCLS health will stay **Degraded** on a non-DRS activated cluster when at least one vCLS VM is not running.

Datastore selection for vCLS VMs

The datastore for vCLS VMs is automatically selected based on ranking all the datastores connected to the hosts inside the cluster. A datastore is more likely to be selected if there are hosts in the cluster with free reserved DRS slots connected to the datastore. The algorithm tries to place vCLS VMs in a shared datastore if possible before selecting a local datastore. A datastore with more free space is preferred and the algorithm tries not to place more than one vCLS VM on the same datastore. You can only change the datastore of vCLS VMs after they are deployed and powered on.

If you want to move the VMDKs for vCLS VMs to a different datastore or attach a different storage policy, you can reconfigure vCLS VMs. A warning message is displayed when you perform this operation.

You can perform a storage vMotion to migrate vCLS VMs to a different datastore. You can tag vCLS VMs or attach custom attributes if you want to group them separately from workload VMs, for instance if you have a specific meta-data strategy for all VMs that run in a data center.

Note: When a datastore is placed in maintenance mode, if the datastore hosts vCLS VMs, you must manually apply storage vMotion to the vCLS VMs to move them to a new location or put the cluster in retreat mode. A warning message is displayed.

```
The enter maintenance mode task will start but cannot finish because there is 1 virtual
 machine residing on the datastore. You can always cancel the task in your Recent Tasks if
 you decide to continue.
```

```
The selected datastore might be storing vSphere Cluster Services VMs which cannot be
 powered off. To ensure the health of vSphere Cluster Services, these VMs have to be
 manually vMotioned to a different datastore within the cluster prior to taking this
 datastore down for maintenance. Refer to this KB article: KB 79892.
```

Select the check box `Let me migrate storage for all virtual machines and continue entering maintenance mode after migration.` to proceed.

Monitoring vSphere Cluster Services

You can monitor the resources consumed by vCLS VMs and their health status.

vCLS VMs are not displayed in the inventory tree in the **Hosts and Clusters** tab. vCLS VMs from all clusters within a data center are placed inside a separate VMs and templates folder named **vCLS**. This folder and the vCLS VMs are visible only in the **VMs and Templates** tab of the vSphere Client. These VMs are identified by a different icon than regular workload VMs. You can view information about the purpose of the vCLS VMs in the **Summary** tab of the vCLS VMs.

You can monitor the resources consumed by vCLS VMs in the **Monitor** tab.

Table 138: vCLS VM Resource Allocation

Property	Size
VMDK size	245 MB (thin disk)
Memory	128 MB
CPU	1 vCPU
Hard disk	2 GB
Storage on datastore	480 MB (thin disk)

Note: Each vCLS VM has 100MHz and 100MB capacity reserved in the cluster. Depending on the number of vCLS VMs running in the cluster, a max of 400 MHz and 400 MB of capacity can be reserved for these VMs.

You can monitor the health status of vCLS in the **Cluster Services** portlet displayed in the **Summary** tab of the cluster.

Table 139: Health status of vCLS

Status	Color Coding	Summary
Healthy	Green	If there is at least one vCLS VM running, the status remains healthy, regardless of the number of hosts in the cluster.
Degraded	Yellow	If there is no vCLS VM running for less than 3 minutes (180 seconds), the status is degraded.
Unhealthy	Red	If there is no vCLS VM running for 3 minutes or more, the status is unhealthy in a DRS enabled cluster.

Maintaining Health of vSphere Cluster Services

vCLS VMs are always powered-on because vSphere DRS depends on the availability of these VMs. These VMs should be treated as system VMs. Only administrators can perform selective operations on vCLS VMs. To avoid failure of cluster services, avoid performing any configuration or operations on the vCLS VMs.

vCLS VMs are protected from accidental deletion. Cluster VMs and folders are protected from modification by users, including administrators.

Only users which are part of the Administrators SSO group can perform the following operations::

- ReadOnly access for vCLS VMs
- Console access to vCLS VMs
- Relocate vCLS VMs to either new storage, compute resource or both using cold or hot migration
- Power off vCLS VMs

Operations that might disrupt the healthy functioning of vCLS VMs:

- Changing the power state of the vCLS VMs
- Resource reconfiguration of the vCLS VMs such as changing CPU, Memory, Disk size, Disk placement
- VM encryption
- Triggering vMotion of the vCLS VMs
- Changing the BIOS
- Removing the vCLS VMs from the inventory
- Deleting the vCLS VMs from disk
- Enabling FT of vCLS VMs
- Cloning vCLS VMs
- Configuring PMem
- Moving vCLS VM to a different folder
- Renaming the vCLS VMs
- Renaming the vCLS folders
- Enabling DRS rules and overrides on vCLS VMs
- Enabling HA admission control policy on vCLS VMs
- Enabling HA overrides on vCLS VMs
- Moving vCLS VMs to a resource pool
- Recovering vCLS VMs from a snapshot

When you perform any disruptive operation on the vCLS VMs, a warning dialog box appears.

Troubleshooting:

The health of vCLS VMs, including power state, is managed by EAM and WCP services. In case of power on failure of vCLS VMs, or if the first instance of DRS for a cluster is skipped due to lack of quorum of vCLS VMs, a banner appears in the cluster summary page along with a link to a Knowledge Base article to help troubleshoot the error state.

Because vCLS VMs are treated as system VMs, you do not need to backup or snapshot these VMs. The health state of these VMs is managed by vCenter services.

Client Interfaces for vSphere

You can access vSphere components through the vSphere Client, the VMware Host Client, and the vSphere Command-Line Interface.

vSphere Client	The vSphere Client, introduced in vSphere 6.5, is an HTML5-based client and is included with vCenter Server. As of vSphere 7.0, the vSphere Web Client has been deprecated. The is the primary interface for connecting to and managing vCenter Server instances.
VMware Host Client	The VMware Host Client is a Web-based application that you can use to manage individual ESXi hosts that are not connected to a vCenter Server system. For more information about the VMware Host Client, see *vSphere Single Host Management - VMware Host Client*.
vSphere Command-Line Interfaces	vSphere supports multiple command-line interfaces for configuring virtual machines, ESXi hosts, and vCenter Server.

vSphere Managed Inventory Objects

In vSphere, the inventory is a collection of virtual and physical objects on which you can place permissions, monitor tasks and events, and set alarms. You can group most inventory objects by using folders to more easily manage them.

All inventory objects, with the exception of hosts, can be renamed to represent their purposes. For example, they can be named after company departments or locations or functions.

Note: Managed object names cannot exceed 214 bytes (UTF-8 encoded).

vCenter Server monitors and manages the following inventory objects:

Data Centers	Unlike folders, which are used to organize specific object types, a data center is an aggregation of all the different types of objects used to work in virtual infrastructure. Within each data center, there are four separate hierarchies. • Virtual machines (and templates) • Hosts (and clusters) • Networks • Datastores
Clusters	A collection of ESXi hosts and associated virtual machines intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit.
Datastores	A virtual representation of physical storage resources in the data center. A datastore is the storage location for virtual machine files. In an on-premises SDDC, these physical storage resources can come from the local SCSI disk of the ESXi host, the Fibre Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays. For both on-premises and cloud SDDCs, vSAN datastores hide the idiosyncrasies of the underlying physical storage and present a uniform model for the storage resources required by virtual machines.
Folders	Folders allow you to group objects of the same type so you can easily manage them. For example, you can use folders to set permissions across objects, to set alarms across objects, and to organize objects in a meaningful way. A folder can contain other folders, or a group of objects of the same type: data centers, clusters, datastores, networks, virtual machines, templates, or hosts. For example, one folder can contain hosts and a folder containing hosts, but it cannot contain hosts and a folder containing virtual machines.
Hosts	The physical computer on which ESXi is installed. All virtual machines run on hosts or clusters.
Networks	A set of virtual network interface cards (virtual NICs), distributed switches or vSphere Distributed Switches, and port groups or distributed port groups that connect virtual machines to each other or to the physical network outside of the virtual data center. You can monitor networks and set permissions and alarms on port groups and distributed port groups.
Resource pools	Resource pools are used to compartmentalize the CPU and memory resources of a host or cluster. Virtual machines run in, and draw their resources from, resource pools. You can create multiple resource pools as direct children of a standalone host or cluster and then delegate control over each resource pool to other individuals or organizations. You can monitor resources and set alarms on them.
Templates	A template is a primary copy of a virtual machine that can be used to create and provision new virtual machines. Templates can have a guest operating system and application software installed. They

	can be customized during deployment to ensure that the new virtual machine has a unique name and network settings.
Virtual machines	A virtualized computer environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same managed host machine concurrently.
vApps	vSphere vApp is a format for packaging and managing applications. A vApp can contain multiple virtual machines.

Optional vCenter Server Components

Optional vCenter Server components are packaged and installed with the base product, but might require a separate license.

Optional vCenter Server features include:

VMware vSphere®vMotion®	Enables you to move running virtual machines from one ESXi host to another ESXi host without service interruption. It requires licensing on both the source and target host. vCenter Server centrally coordinates all vSphere vMotion activities.
vSphere® Storage vMotion®	Allows you to move the disks and configuration file of a running virtual machine from one datastore to another without service interruption. It requires licensing on the virtual machine's host.
VMware vSphere® High Availability	Enables a cluster with High Availability. If a host fails, all virtual machines that were running on the host are promptly restarted on different hosts in the same cluster. When you enable the cluster for vSphere HA, you specify the number of hosts you want to be able to recover. If you specify the number of host failures allowed as **1**, vSphere HA maintains enough capacity across the cluster to tolerate the failure of one host. All running virtual machines on that host can be restarted on remaining hosts. By default, you cannot turn on a virtual machine if doing so violates required failover capacity.
VMware vSphere®Distributed Resource Scheduler ™	Helps improve resource allocation and power consumption across all hosts and resource pools. vSphere DRS collects resource use information for all hosts and virtual machines in the cluster and gives recommendations (or migrates virtual machines) in one of two situations: • Initial placement – When you power on a virtual machine in the cluster for the first time, DRS either places the virtual machine or makes a recommendation. • Load balancing – DRS attempts to improve resource use across the cluster by performing automatic migrations of virtual machines (vSphere vMotion) or by providing a recommendation for virtual machine migrations. vSphere DRS includes VMware vSphere®Distributed Power Management ™ (DPM) capabilities. When DPM is enabled, the system compares cluster-level and host-level capacity to the demands of virtual machines that are running in the cluster. Based on the results of the comparison, DPM recommends (or implements) actions that can reduce the power consumption of the cluster.
VMware vSphere®Storage DRS™	Allows you to manage multiple datastores as a single resource, called a datastore cluster. A datastore cluster is an aggregation of multiple datastores into a single logical, load-balanced pool. You can treat the datastore cluster as a single flexible storage

	resource for resource management purposes. You can assign a virtual disk to a datastore cluster, and vSphere Storage DRS finds an appropriate datastore for it. The load balancer takes care of initial placement and future migrations based on workload measurements. Storage space balancing and I/O balancing minimize the risk of running out of space and the risk of I/O bottlenecks slowing the performance of virtual machines.
VMware vSphere® Fault Tolerance	vSphere Fault Tolerance provides continuous availability for virtual machines by creating and maintaining a Secondary VM that is identical to the Primary VM. This Secondary VM is continuously available to replace the Primary VM in a failover situation.

vCenter Server Plug-Ins

vCenter Server plug-ins extend the capabilities of vCenter Server by providing additional features and functions.

Some plug-ins are installed as part of the base vCenter Server product.

vCenter Storage Monitoring	Allows you to review information on storage use and to map relationships visually between all storage entities available in vCenter Server.
vCenter Hardware Status	Uses CIM monitoring to display the hardware status of hosts that vCenter Server manages.
vCenter Service Status	Displays the status of vCenter services.

Some plug-ins are packaged separately from the base product and require separate installation. You can update plug-ins and the base product independently of each other. VMware modules include:

vSphere Lifecycle Manager	Enables administrators to apply updates and patches across ESXi hosts and all managed virtual machines. Administrators can create user-defined security baselines that represent a set of security standards. Security administrators can compare hosts and virtual machines against these baselines to identify and remediate systems that are not in compliance.
vRealize Orchestrator	A workflow engine that enables you to create and run automated workflows in your vSphere environment. vRealize Orchestrator coordinates workflow tasks across multiple VMware products and third-party management and administration solutions through its open plug-in architecture. vRealize Orchestrator provides a library of workflows that are extensible. You can use any operation available in the vCenter Server API to customize vRealize Orchestrator workflows.

Using the vSphere Client

Use the vSphere Client to connect to vCenter Server systems and manage vSphere inventory objects.

Use of the vSphere Client requires a supported Web browser.

The home screen of the vSphere Client is a system dashboard that aggregates data from different sources in the environment together in a single, unified view.

VMware has tested and supports the following guest operating systems and browser versions for the vSphere Client.

Table 140: Supported Guest Operating Systems and Browser Versions for the vSphere Client.

Operating system	Browser
Windows 32-bit and 64-bit	Microsoft Edge: 89 or later. Mozilla Firefox: 80 or later. Google Chrome: 90 or later.
Mac OS	Microsoft Edge: 89 or later. Mozilla Firefox: 80 or later. Google Chrome: 90 or later.

Later versions of these browsers are likely to work, but have not been tested.

Log In to vCenter Server by Using the vSphere Client

You can use the vSphere Client to log in to vCenter Server and manage your vSphere inventory.

The vSphere Client is automatically installed as part of the vCenter Server appliance deployment. This way, the vSphere Client always points to the same vCenter Single Sign-On instance.

1. Open a Web browser and enter the URL for your vCenter Server instance:
   `https://vcenter_server_ip_address_or_fqdn`
   As an alternative, you can open a Web browser and enter the URL for the vSphere Client:
   `https://vcenter_server_ip_address_or_fqdn/ui`.
2. If a warning message about a potential security risk appears, select to continue to the website.

Browser	Action
Microsoft Edge	1. Click **Details**. 2. Under the additional message that appears, click **Go on to the webpage**.
Mozilla Firefox	1. Click **Advanced**. 2. Under the additional message that appears, click **Accept the Risk and Continue**.
Google Chrome	1. Click **Advanced**. 2. Under the additional message that appears, click **Proceed to *vcenter_server_ip_address_or_fqdn***.

3. On the vSphere Welcome page, select **Launch vSphere Client (HTML5)**.
4. If the warning message about a potential security risk appears again, repeat Step 2.
5. Enter the credentials of a user who has permissions on vCenter Server and click **Login**.

The vSphere Client connects to all the vCenter Server systems on which the specified user has permissions, and you can view and manage the vSphere inventory.

Manage the Login Message to the vSphere Client Login Page

You can add a login message to the vSphere Client login page. You can also configure a custom login message and provide a check box for user consent.

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.
   If you specified a different domain during installation, log in as administrator@*mydomain*.

3. Navigate to the Configuration UI.
   a) From the **Home** menu, select **Administration**.
   b) Under **Single Sign On**, click **Configuration**.
4. Click the **Login Message** tab.
5. Click **Edit** and configure the login message.

Option	Description
Show login message	Toggle on **Show login message** to enable the login message. You cannot make changes to the login message unless you toggle on this switch.
Login message	Title of the message. By default, when **Consent checkbox** is toggled on, the login message text is `I agree to Terms and Conditions.` You must replace `Terms and Conditions` with your own text. If the **Consent checkbox** is toggled off, then `Login message` appears, over which you enter your message.
Consent checkbox	Toggle on **Consent checkbox** to require that the user clicks a check box before logging in. You can also display a message without a check box.
Details of login message	Message that the user sees when clicking the login message, for example, the text of the terms and conditions. You must enter some details in this text box.

6. Click **Save**.

Navigate the vSphere Inventory by Using the Global Inventory Lists Navigator

You can use the **Global Inventory Lists** navigator to browse and select objects in the vSphere inventory as an alternative to the hierarchical inventory tree.

Unlike the inventory tree, which presents hierarchical arrangements of the parent and the child objects arranged in the **Hosts and Clusters**, **VMs and Templates**, **Storage**, and **Networking** inventory lists, the Global Inventory Lists navigator presents a list of all related objects in the inventory. You can navigate from an object to its related objects, regardless of their type.

Tip:

You can retrieve all objects of a specific type by using the vSphere Web Services API and the vSphere Automation API. For more information about how to use the APIs, see the *vSphere Web Services SDK Programming Guide* and the *vSphere Automation Programming Guides* at https://developer.broadcom.com/.

1. From the vSphere Client home page, click **Global Inventory Lists**.
2. In the left pane, select one of the object or the resource categories to view the objects of that type.
   For example, to view the hosts in the vSphere inventory, click **Hosts**.
3. In the left navigation pane, to display information about the object, click an object from the list once.
4. Optional: Click the object again to open it.

   Opening an object brings it to the top of the navigator and displays related object categories beneath it.

   For example, opening a host allows you to see the child resource pools, virtual machines, datastores, networks, and distributed switches associated with this host.
5. To access additional information or manage the selected object, click one of the tabs in the center pane.

Option	Description
Summary	You can view basic status and configuration for an object.
Monitor	You can view alarms, performance data, resource allocation, events, and other status information for an object.
Configure	Depending on the selected object, you can edit settings, alarm definitions, tags, permissions, and so on.

Option	Description
Permissions	You can view, add, change, and delete permissions. This tab is only available for logged in users with administration privileges.
Related Objects tabs	You can view and manage the objects related to the object that you selected. For example, if you select a host, the tabs that you see are **VMs**, **Resource Pools**, **Datastores**, and **Networks**.
Updates	Depending on the selected object, you can check the hardware compatibility of a host against the VMware Compatibility Guide, check the status of virtual machines, upgrade the VMware Tools version or the virtual hardware version of the virtual machines, and perform vSphere Lifecycle Manager operations. **Note:** The **Updates** tab is available only for certain types of inventory objects, for example, hosts, virtual machines, and clusters.

Manage Client Plug-Ins

With Client Plug-In Management you can monitor plug-in downloads, deployments, upgrades, and undeployments.

From the vSphere Client, you can monitor vCenter Server client plug-ins using the **Recent Tasks** pane, the global **Tasks** view, or the **Administration** > **Client Plugins** view. In addition to monitoring installation progress, you can troubleshoot installation failures and plug-in incompatibilities. You can also activate and deactivate installed plug-ins.

Monitor Client Plug-Ins

You can monitor plug-in activities including installation progress, failures, deployments, upgrades, and undeployments. You can also activate or deactivate client plug-ins.

1. In the vSphere Client home page, click **Administration** > **Solutions** > **Client Plugins**.

   The Client Plugins Table shows detailed plug-in information, including version, enablement status, and deployment status.
2. Optional: To see more information about failed or incompatible deployments, click the status message.
3. Optional: Activate or deactivate a client plug-in.
   a) Select the radio button next to the plug-in.
   b) Click **Enable** or **Disable**.
   c) Click **Yes**.

Refresh Data

You must manually refresh the data in the vSphere Client to see changes made to objects by other users during your session.

For performance reasons, the vSphere Client does not continuously refresh data on all objects in the inventory. All changes that you make during your current session are immediately reflected in the client user interface. Change made by other users or in other sessions are not reflected until you manually refresh the data.

To update all data in the current vSphere Client view, click the refresh icon ( ).

The client view is updated.

Searching the Inventory

With the vSphere Client, you can search the inventory for objects that match specified criteria. You can search the inventories of all vCenter Server systems.

You can only view and search for inventory objects that you have permission to view.

Note: If your permissions change while you are logged in, the search service might not immediately recognize these changes. To ensure that your search is performed with up-to-date permissions, log out of all your open sessions and log in again before you perform the search.

Perform a Quick Search

A quick search checks all types of objects for the specified search term within the name or other properties of the object.

1. Enter the search term in the search box at the top of the vSphere Client window.

   Multiple search terms in a quick or simple search are treated as if they are connected by ORs. For example, searching for `example machine` finds all objects with names containing either "example" or "machine".

   The search results appear below the search box as you type. The number of items displayed is limited to 10.
2. Optional: To run a saved search, click the saved search icon and select a saved search query.
3. Optional: To display an item in the inventory, click the item from the drop-down list of the search results.
4. Optional: To see more search results or more details about the search results, click the summary of the search results from the drop-down list of search results.

   a) Optional: To display an object in the inventory, click the object in the search results page.

   The search results are listed in tables arranged by object type. For example, if a search finds hosts and virtual machines, the following tables appear: **Hosts**, which shows only host results and **Virtual Machines**, which shows only virtual machine results.

Related Links

Save a Search on page 1748
You can save search queries in the vSphere Client so you can rerun, rename, or delete them later.

Manage a Saved Search on page 1749
In the vSphere Client, you can rename, delete, or create a duplicate of a saved search query.

Save a Search

You can save search queries in the vSphere Client so you can rerun, rename, or delete them later.

1. In a vSphere Client window, enter a query for a simple search in the search box.
2. Click the summary of the search results from the drop-down list with search results.
3. On the search results page, click **Save Search**.
4. Enter a name for the search query. Names must be lowercase with no spaces.
5. Click **Save**.

   The search query you entered is saved. You can reload the query later and repeat the search.

Related Links

Perform a Quick Search on page 1748
A quick search checks all types of objects for the specified search term within the name or other properties of the object.

Manage a Saved Search on page 1749
In the vSphere Client, you can rename, delete, or create a duplicate of a saved search query.

Manage a Saved Search

In the vSphere Client, you can rename, delete, or create a duplicate of a saved search query.

1. At the top of the vSphere Client window, click inside the search box.
2. Click the saved search icon and select a saved search query.
3. On the Search Results page, click **Actions** and select one of the options:

Option	Description
Save as	Creates a duplicate of the saved search query.
Rename	Renames the saved search query.
Delete	Deletes the saved search query.

4. Confirm the changes.

Related Links

Perform a Quick Search on page 1748

A quick search checks all types of objects for the specified search term within the name or other properties of the object.

Save a Search on page 1748

You can save search queries in the vSphere Client so you can rerun, rename, or delete them later.

Sort the vSphere Client Inventory

You can use sortable columns and input filters to sort and find objects in your vSphere Client inventory that meet certain criteria.

You can sort list views by column. These list views can be selected in the **Global Inventory Lists** pane or found in search results.

From a list view, you can use the **Filter** field to filter objects.

For example, you can sort virtual machines by name, provisioned space, used space, and so on. You can filter them by name, state, status, and so on.

1. In the vSphere Client home page, select **Global Inventory Lists**.
2. To open an object list view, select an object type from the list.

   If objects from the selected type are not present in the inventory, a blank page appears.
3. Optional: Click the column you want to sort objects by. You can click again on that column to reverse the sorting order.
4. Add or remove columns from the object list view:
   a)

      Click the **Pick columns** icon ( ) at the bottom left corner of the object list view.

      The **Show Columns** pop-up appears.
   b) Optional: To show a column in the object list view, select the check box for the column from the list.
   c) Optional: To hide a column from the object list view, deselect the check box for the column from the list.
5. Optional: To filter the inventory objects, enter your filtering parameter in the filter field in the right upper corner of the inventory object list table. For example, in the virtual machine list view, to filter for all virtual machines that are in a powered on state, you must type `powered on`.

   A list of inventory objects that meet your filtering criteria is displayed in your selected sorting order.

After you apply a filter to an object list, the filter is active during the login session. To clear the filtered list of inventory objects, delete the filter criteria from the filter field.

Drag Objects

You can select an inventory object, and while holding the left mouse button you can drag it to another object. Drag is an alternative way to initiate operations that are available in the context menu, such as **Move To** and **Migrate**.

For completing some drag operations, you do not need to perform any additional actions. For completing others, you might have to go through a wizard.

1. On the vSphere Client home page, select an inventory list.
   The inventory tree appears.
2. Select the object to move and drag it to a destination object.
   The mouse pointer changes depending on whether you can drop the object to the object you currently point to.

Table 141: Mouse Icons Indicating Possible Drag Operations

Icon	Description
	You can drop the object that you are dragging into this object.
	You cannot drop the object that you are dragging into this object.

3. Drop the object on the destination object.
   A task starts in the Recent Tasks pane.
4. If a wizard opens, follow the prompts to complete the drag operation.

The object is moved to the destination object that you selected.

Keyboard Shortcuts

Keyboard shortcuts allow you to navigate quickly or perform a task in the vSphere Client.

Inventory Keyboard Shortcuts

With inventory keyboard shortcuts you can quickly navigate to different inventories in the vSphere Client.

Table 142: Inventory Keyboard Shortcuts

Keyboard Combination on a Windows machine	Keyboard Combination on a Mac machine	Action
Ctrl+Alt+Home	Control+Option+Home	Home
Ctrl+Alt+1	Control+Option+1	Shortcuts
Ctrl+Alt+2	Control+Option+2	Hosts and Clusters
Ctrl+Alt+3	Control+Option+3	VMs and Templates
Ctrl+Alt+4	Control+Option+4	Storage
Ctrl+Alt+5	Control+Option+5	Networking
Ctrl+Alt+6	Control+Option+6	Content Libraries
Ctrl+Alt+7	Control+Option+7	Workload Management
Ctrl+Alt+8	Control+Option+8	Global Inventory Lists
Ctrl+Alt+R	Control+Option+R	Refresh

Keyboard Combination on a Windows machine	Keyboard Combination on a Mac machine	Action
Ctrl+Alt+S repeat twice	Control+Option+S repeat twice	Search

Export Lists

You can export the contents of an inventory list view to a CSV file.

1. In the vSphere Client, click **Menu** and select **Global Inventory Lists**.
2. In the left pane, select one of the object or resource categories to view objects of that type.
   For example, click **Hosts** to view the hosts in the vSphere inventory.
3. Select whether you want all columns or your current selection of columns to be listed in the CSV file.
   a)
   Click the **Pick columns** icon ( ) at the bottom left corner of the object list view.
   The **Show Columns** pop-up appears.
   b) Optional: To show a column in the object list view, select the check box for the column from the list.
   c) Optional: To hide a column from the object list view, deselect the check box for the column from the list.
   d) Optional: To show all columns, click **Select All**.
4. Click the **EXPORT** option at the bottom left corner of a list view and select whether you want all rows or your currently selected rows to be listed in the CSV file.
   By default, if you do not select objects from the list, the information about all listed objects is exported.

The CSV file is generated and available for download.

Configure the vSphere Client Timeout Value

By default, the vSphere Client sessions close after 120 minutes of idle time, requiring the user to log in again to resume using the client. You can change the timeout value by editing the `webclient.properties` file.

You can configure the timeout of the vSphere Client by changing the value of the `session.timeout` property in the `webclient.properties` file.

Edit the Properties File of the vSphere Client

1. On the computer where the vSphere Client is installed, navigate to the `/etc/vmware/vsphere-ui` file path where the `webclient.properties` file is located.
2. Edit the file to include the line `session.timeout = <custom_value>`, where `<custom_value>` is the timeout value in minutes. Uncomment the line, if necessary.
   To set the client to never timeout, specify a negative or `0` value for the timeout.
   For example, to set the timeout value to 60 minutes, include the line `session.timeout = 60`.
3. Restart the VMware vSphere Client service.

Change the Client Configuration in the vSphere Client

1. In the vSphere Client, navigate to **Home** > **Administration**.
2. Under **Deployment**, select **Client Configuration**.
3. In the **Client Configuration** pane, click **Edit**.
   The **Edit client configuration** dialog box appears.

4. Enter a new value in minutes in the session timeout text box.
5. Click **Save**.
6. Restart the VMware vSphere Client service.

Attach File to Service Request

You can attach files, such as log files or screenshots, to VMware Service Requests directly from the vSphere Client.

If you already have a Service Request ID with VMware, you can use the vSphere Client to upload the system log bundles directly to your service request.

1. From the vSphere Client sidebar, click **Administration**.
2. In the Administration panel, under Support, click **Upload File to Service Request**.
3. Click the **Upload File to Service Request** button.
4. Enter the Service Request ID.
5. Click **Browse** and select the file to attach.
6. Click **Upload**.

Provide Feedback with the vSphere Client

You can use the improved feedback tool in the vSphere Client to provide timely feedback to our developers.

1. From the vSphere Client home screen, click the feedback icon in the top right corner.
2. Select the type of feedback you want to give and enter your feedback in the **Description** window.
3. Optional: Provide an email address and screenshots or other images.
4. Click **Send**.

Start, Stop, and Restart Services

In the vSphere Client, you can start, stop, and restart services that are running on vCenter Server. You can restart services upon a configuration change or for suspected functional or performance issues.

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

1. Log in to the vCenter Server Management Interface.
   - Log in to the vCenter Server Management Interface directly.
   - In the vSphere Client home page, select **Administration** > **System Configuration**. Click a node from the list.
2. On the vCenter Server Management Interface home page, click **Services**.
3. Select a service from the service list.
4. From the top menu, click **Restart**, **Start**, or **Stop**.

   Unavailable options are dimmed.

   Note: Restarting the Content Library Service also restarts the Transfer Service and the OVF Service. The Content Library Service, the Transfer Service, and the OVF Service run on the same Tomcat server.

Submit Suggestions for New Features and Feature Requests Through the vSphere Ideas Portal

You can provide suggestions for new features or share feature requests through the vSphere Ideas portal. Al users with valid Broadcom Support Portal accounts can access the vSphere Ideas portal.

Verify that you have a valid Broadcom Support Portal account.

The vSphere Ideas portal is public. When you publish new ideas and feature requests, consider whether you want to share personal data.

You can access the vSphere Ideas portal directly by going to https://vsphere.ideas.aha.io/ and entering a valid Broadcom Support Portal user name and password.

Alternatively, you can access the vSphere Ideas portal by using the vSphere Client.

1. On the vSphere Client home page, click the feedback iconin the top-right corner.
2. In the **Send Feedback** dialog box, click **Idea**.
3. Click **Visit ideas portal**.
4. On the Broadcom Support Portal login page, enter a valid user name and password.
   You are redirected to https://vsphere.ideas.aha.io/ .
5. On the vSphere Ideas portal home page, click **Add a new idea**.
6. On the **Add a new idea** page, enter the details about your idea and click **Share idea**.

Your idea appears in the **Recent** tab. All users of the vSphere Ideas portal can view, subscribe, vote, and comment on your idea.

Using Enhanced Linked Mode

Enhanced Linked Mode links multiple vCenter Server systems. With Enhanced Linked Mode, you can view and search across all linked vCenter Server systems. This mode replicates roles, permissions, licenses, and other key data across systems.

Enhanced Linked Mode provides the following features for vCenter Server:

- You can log in to all linked vCenter Server systems simultaneously with a single user name and password.
- You can view and search the inventories of all linked vCenter Server systems within the vSphere Client.
- Roles, permission, licenses, tags, and policies are replicated across linked vCenter Server systems.

To join vCenter Server systems in Enhanced Linked Mode, connect them to the same vCenter Single Sign-On domain.

For more information about vCenter Enhanced Linked Mode, see the *vCenter Server Installation and Setup* guide.

Configuring Customer Experience Improvement Program

You can participate in the Customer Experience Improvement Program (CEIP) to provide anonymous feedback or information to VMware for quality, reliability, and functionality improvments of VMware products and services.

VMware Customer Experience Improvement Program

VMware Tools participates in VMware's Customer Experience Improvement Program (CEIP).

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Join or Leave Customer Experience Improvement Program in vSphere Client

You can join your vCenter Server to the Customer Experience Improvement Program (CEIP), or decide to leave the CEIP at any time. To leave and rejoin your host to the CEIP, see *vSphere Single Host Management - VMware Host Client* documentation.

Obtain the user name and password of the administrator account.

1. From the vSphere Client login page, log in to vCenter Server by using the credentials of the administrator account.
2. On the vSphere Client home page, click **Administration**.
3. Under Deployment, click **Customer Experience Improvement Program**
4. Click **Join** to join the CEIP or **Leave CEIP** to leave the Program.

Organizing Your Inventory

Plan how to set up your virtual inventory and consider how the virtual machines that it will support are going to be used and administered. A large vSphere implementation might contain several virtual data centers with a complex arrangement of hosts, clusters, resource pools, and networks. It might involve multiple vCenter Server systems connected using Enhanced Linked Mode. Smaller implementations might require a single virtual data center with a much less complex topology.

Here are the questions to answer as you create and organize an inventory of virtual objects:

- Will some virtual machines require dedicated resources?
- Will some virtual machines experience periodic spikes in workload?
- Will some virtual machines need to be administered as a group?
- Will some virtual objects require one set of system permissions, while other objects will require a different set of permissions?
- Do you want to use multiple vSphere Standard Switches, or you want to have a single vSphere Distributed Switch per data center?
- Do you want to use vMotion and Distributed Resource Management with certain virtual machines but not others?

The left pane of the vSphere Client displays your vSphere inventory. You can add and arrange objects in any way with the following considerations:

- The name of an inventory object must be unique with its parent.
- vApp names must be unique within the Virtual Machines and Templates view.
- System permissions are inherited and cascade. When you assign a system permission to an object in the inventory, the same permission propagates down the object hierarchy.

Tasks for Organizing Your Inventory

Populating and organizing your inventory involves the following activities:

Note: vCenter Server supports an 80 character limit for all its entities. When you create a new inventory object, if the name exceeds this limit, the task fails and a warning appears.

- Creating data centers.
- Adding hosts to the data centers.
- Organizing inventory objects in folders.
- Setting up networking by using vSphere Standard Switches or vSphere Distributed Switches. To use services such as vMotion, TCP/IP storage, VMware vSAN™, and Fault Tolerance, setup VMkernel networking for these services. For more information, see *vSphere Networking*.

- Configuring storage systems and creating datastore inventory objects to provide logical containers for storage devices in your inventory. See *vSphere Storage*.
- Creating clusters to consolidate the resources of multiple hosts and virtual machines. You can enable vSphere HA and vSphere DRS for increased availability and more flexible resource management. See *vSphere Availability* for information about configuring vSphere HA, and *vSphere Resource Management* for information about configuring vSphere DRS.
- Creating resource pools to provide logical abstraction and flexible management of the resources in vSphere. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. See *vSphere Resource Management* for details.

Create a Data Center

A virtual data center is a container for all the inventory objects required to complete a fully functional environment for operating virtual machines. You can create multiple data centers to organize groups of environments to meet different user needs. For example, you can create a data center for each organizational unit in your enterprise or create some data centers for high-performance environments and other data centers for less demanding environments.

Required privileges:

- **Datacenter** > **Create datacenter**

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Right-click the vCenter Server object and select **New Datacenter**.
3. Optional: Enter a name for the data center and click **OK**.

Add hosts, clusters, resource pools, vApps, networking, datastores, and virtual machines to the data center.

Create a Folder

You can use folders to group objects of the same type for easier management. For example, you can apply a common set of permissions to the folder and these permissions apply to all objects grouped in the folder.

A folder can contain other folders, or a group of objects of the same type. For example, one folder can contain both virtual machines and another folder that contains virtual machines, but it cannot contain both hosts and a folder that contains virtual machines.

1. In the vSphere Client, select either a data center or another folder as a parent object for the folder that you want to create.
2. Right-click the parent object and click **New Folder**.
   - If the parent object is a folder, the new folder is of the same type as the parent folder - it can contain only objects of the same type that the parent folder contains.
   - If the parent object is a data center, you can create one of four types of folders: **Host and Cluster** folders, **Network** folders, **Storage** folders, and **VM and Template** folders.
3. Enter a name for the folder and click **OK**.

Move objects into the folder by right-clicking the object and selecting **Move To**. Select the folder as the destination. You can also move an object by dragging it to the destination folder.

Add a Host to a Folder or a Data Center

You can add hosts under a data center object, a folder object, or a cluster object. If a host contains virtual machines, those virtual machines are added under the host in the inventory.

- Verify that a data center or a folder exists in the inventory.

- Obtain the user name and password of the root user account for the host.
- Verify that hosts behind a firewall are able to communicate with the vCenter Server system and all other hosts through port 902 or another custom-configured port.
- Verify that all NFS mounts on the host are active.
- Verify that you have the proper privileges. Different sets of privileges apply when you add multiple hosts to a cluster and a single host to a cluster or a data center. For more information, see Required Privileges for Common Tasks in the *vSphere Security* documentation.
- If you want to add a host with more than 512 LUNs and 2,048 paths to the vCenter Server inventory, verify that the vCenter Server instance is suitable for a large or an x-large environment.

1. In the vSphere Client, navigate to a data center or folder within a data center.
2. Right-click the data center or folder and select **Add Host**.
3. Enter the IP address or the name of the host and click **Next**.
4. Enter administrator credentials and click **Next**.
5. Review the host summary and click **Next**.
6. License the host through one of the following methods.
   - Assign an already existing license.
   - Assign a new license.
7. In the Add Host wizard, click **Next**.
8. Optional: Select a lockdown mode option to deactivate the remote access for the administrator account after vCenter Server takes control of this host and click **Next**.
9. Optional: If you add the host to a data center or a folder, select a location for the virtual machines that reside on the host and click **Next**.
10. Review the summary and click **Finish**.

A new task for adding the host appears in the Recent Tasks pane. It might take a few minutes for the task to complete.

Creating and Configuring Clusters

A cluster is a group of hosts. When a host is added to a cluster, the resources of the host become part of the resources of the cluster. The cluster manages the resources of all hosts that it contains.

Starting with vSphere 6.7, you can create and configure a cluster that is hyper-converged. The hyper-converged infrastructure collapses compute, storage, and networking on a single software layer that runs on industry standard x86 servers.

You can create and configure a cluster by using the simplified Quickstart workflow in the vSphere Client. On the **Cluster quickstart** page, there are three cards for configuring your new cluster.

Table 143: The cards initiating wizards for renaming and configuring a new cluster

Cluster Quickstart Workflow	Description
1. Cluster basics	You can edit the cluster name and activate or deactivate cluster services. The card lists the services you enabled.
2. Add hosts	You can add new ESXi hosts. After the hosts are added, the card shows the total number of hosts present in the cluster and displays health check validation for those hosts.

Cluster Quickstart Workflow	Description
3.Configure cluster	You can configure network settings for vMotion traffic, review and customize cluster services. After the cluster is configured, the card provides details on configuration mismatch and reports cluster health results through the vSAN Health service.

The **Skip Quickstart** button prompts you to continue configuring the cluster and its hosts manually. To confirm exiting the simplified configuration workflow, click **Continue**. After you dismiss the **Cluster quickstart** workflow, you cannot restore it for the current cluster.

If you plan to enable vSphere High Availability (HA), vSphere Distributed Resource Scheduler (DRS), and the VMware vSAN features, you must create clusters.

Starting with vSphere 7.0, you can create a cluster that you manage with a single image. By using vSphere Lifecycle Manager images, you can easily update and upgrade the software and firmware on the hosts in the cluster. Starting with vSphere 7.0 Update 2, during cluster creation, you can select a reference host and use the image on that host as the image for the newly created cluster. For more information about using images to manage ESXi hosts and clusters, see the *Managing Host and Cluster Lifecycle* documentation.

Starting with vSphere 7.0 Update 1, vSphere Cluster Services (vCLS) is enabled by default and runs in all vSphere clusters. vCLS ensures that if vCenter Server becomes unavailable, cluster services remain available to maintain the resources and health of the workloads that run in the clusters. For more information about vCLS, see vSphere Cluster Services.

Create a Cluster

You create a new and empty cluster object by using the Quickstart workflow in the vSphere Client.

- Verify that a data center, or a folder within a data center, exists in the inventory.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.
- To create a cluster that you manage with a single image, review the requirements and limitations information in the *Managing Host and Cluster Lifecycle* documentation.

Required privileges:

- **Host** > **Inventory** > **Create cluster**

Starting with vSphere 7.0, the clusters that you create can use vSphere Lifecycle Manager images for host updates and upgrades.

A vSphere Lifecycle Manager image is a combination of vSphere software, driver software, and desired firmware with regard to the underlying host hardware. The image that a cluster uses defines the full software set that you want to run on the ESXi hosts in the cluster: the ESXi version, additional VMware-provided software, and vendor software, such as firmware and drivers.

The image that you define during cluster creation is not immediately applied to the hosts. If you do not set up an image for the cluster, the cluster uses baselines and baseline groups. Starting with vSphere 7.0 Update 2, during cluster creation, you can select a reference host and use the image on that host as the image for the newly created cluster. For more

information about using images and baselines to manage hosts in clusters, see the *Managing Host and Cluster Lifecycle* documentation.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a data center.
3. Right-click the data center and select **New Cluster**.
4. Enter a name for the cluster.
5. Select DRS, vSphere HA, or vSAN cluster features.

Option	Description
To use DRS with this cluster	1. Slide the switch to the right to enable the DRS service. 2. Click the info icon on the left to see the **Default Settings** for the DRS service. The default values are: – Automation Level: Fully Automated Migration – Threshold: 3
To use vSphere HA with this cluster	1. Slide the switch to the right to enable the vSphere HA service. 2. Click the info icon on the left to see the **Default Settings** for the vSphere HA service. You are present with the following default values: Host Monitoring: Enabled Admission Control: Enabled VM Monitoring: Disabled
To use vSAN with this cluster	• Slide the switch to the right to enable the vSAN service. For more information on vSAN, see Creating a vSAN Cluster in the *vSAN Planning and Deployment* documentation.

   You can override the default values later on in the workflow.
6. Optional: To create a cluster that you manage with a single image, select the **Manage all hosts in the cluster with a single image** check box.

   For information about creating a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.
7. Click **Next**.
8. Review the cluster details and click **Finish**.

   The cluster appears in the vCenter Server inventory. The **Quickstart** service appears under the **Configure** tab.
9. Optional: To rename your cluster and to activate or deactivate cluster services, click **Edit** in the **Cluster basics** card.

You have created an empty cluster in the vCenter Server inventory.

Add hosts to the cluster.

Add a Host to a Cluster

You can add new and existing ESXi hosts to the vCenter Server inventory.

- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.

- Verify that you have the proper privileges. Different sets of privileges apply when you add multiple hosts to a cluster and a single host to a cluster or a data center. For more information, see Required Privileges for Common Tasks in the *vSphere Security* documentation.
- To add a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

You can also add hosts to a DRS cluster. For more information, see *vSphere Resource Management*.

When you add the first three hosts to the cluster, vSphere Cluster Services (vCLS) agent virtual machines are added by default to the cluster. A quorum of up to three vCLS agent virtual machines are required to run in a cluster, one agent virtual machine per host. For more information about vCLS, see vSphere Cluster Services.

Note: After you configure the cluster by using Quickstart, if you modify any cluster networking settings outside of Quickstart, you cannot use the Quickstart workflow to add and configure new hosts to the cluster.

1. In the vSphere Client, navigate to a cluster within a data center.
2. On the **Configure** tab, select **Configuration** > **Quickstart**.
3. Click **Add** in the **Add hosts** card.
4. On the **Add hosts** page, add new or existing hosts to the cluster.
   - Add hosts that are not part of the vCenter Server inventory.
     a. Click the **New hosts** tab.
     b. Populate the IP Address and credentials text boxes for those hosts.
     c. To add more new hosts, click the **Add Host** button.
     d. To reuse the credentials for all added hosts, select the **Use the same credentials for all hosts** check box.
   - Add hosts that are managed by your vCenter Server instance and are in the same data center as your cluster.
     a. Click the **Existing hosts** tab.
     b. From the list, select the hosts that you want to add to the cluster.
5. Click **Next**.

   The **Host summary** page lists all hosts that will be added to the cluster and related warnings.

   Note: If a host cannot be validated automatically by the system, you are prompted to manually validate its certificate and accept its thumbprint in the **Security Alert** pop-up.
6. On the **Host summary** page, review the details of the added hosts and click **Next**.
7. Optional: On the **Import Image** page, select the host whose image to use as the image for the cluster.

   The **Import Image** page appears when you add hosts to a cluster managed with a single image. For information about adding a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.
8. On the **Ready to complete** page, review the IP addresses or FQDN of the added hosts and click **Finish**.

   Review the number of added hosts and the health check validation, performed by the vSAN Health service, in the **Add hosts** card.
9. Optional: Click **Re-validate** to retrigger the validation of the hosts.

   Note: If an error occurs, it is visible in the **Recent Tasks** pane only.

All hosts are placed in maintenance mode and added to your cluster. You can manually exit the maintenance mode.

Configure your cluster default settings through the Quickstart workflow.

Configure a Cluster

To configure the host networking settings on your host and to customize the cluster settings, start the **Configure cluster** wizard, part of the Cluster quickstart workflow.

1. In the vSphere Client, navigate to a cluster.
2. On the **Configure** tab, select **Configuration** > **Quickstart**.

   The **Cluster quickstart** page appears.

   Note:

   To configure your cluster host networking and services manually by referring to different parts of the vSphere software, click the **Skip quickstart** button. If you dismiss the **Cluster quickstart** workflow, you cannot restore it, and you have to configure manually any hosts that you add to this cluster in the future.
3. In the **Configure hosts** card, select **Configure**.
4. On the **Distributed switches** page, configure the cluster networking.

   Alternatively, you can select the Configure networking settings later check box to configure the default settings only for the cluster services and to hide all options that are related to host networking.

   CAUTION:

   After you select the Configure networking settings later check box, and complete the **Configure cluster** workflow, you cannot perform the networking configuration in the future by using the **Configure cluster** wizard.

   a) Specify the number of distributed switches to create from the drop-down menu.

      Note: You can select up to three distributed switches.

      The selected distributed switches are configured as part of this workflow and all hosts in the cluster connect to them.
   b) Enter a unique name for each of the distributed switches you are about to create.
   c) Optional: Click **Use Existing** to select an existing compatible distributed switch and an existing compatible distributed port group.
   d) To set up the vMotion network, select a distributed switch from the drop-down menu and assign a new default port group to it.
   e) In the **Physical adapters** section, for each physical network adapter (NIC), select the distributed switch name from the drop-down menu.

      The new distributed switch must be assigned to at least one physical adapter.

      Note: If you are using an existing distributed switch, the physical adapter selection must match the current mapping of the distributed switch. Any variation results in an error.

      This mapping of physical NICs to the distributed switches is applied to all hosts in this cluster.
   f) Click **Next**.
5. If the vSphere DRS feature is enabled on the cluster, configure the networking options in the vMotion traffic page.
   a) Optional: Select the **Use VLAN** check box and enter an ID for the vMotion distributed port group.
   b) Optional: Select a protocol type from the drop-down menu.
   c) Select an IP type from the drop-down menu.
   d) Optional: Populate the text boxes for each host in the cluster depending on the IP address type you need for setting up the networking.

      If the IP address type is set to `DHCP`, these text boxes are dimmed.
6. Click **Next**.

   The **Advanced options** page appears.

7. Optional: If you enabled the vSphere HA feature during cluster creation, use the options in the **High Availability** section to activate or deactivate host failure monitoring, virtual machine monitoring, and admission control.

   If you enable admission control, you can specify the failover capacity by number of hosts.

8. Optional: If you enabled the vSphere DRS feature during cluster creation, the **Distributed Resource Scheduler** section is visible.
   a) Set the Automation level to Fully Automated, Partially Automated or Manual.
   b) Select one of the five migration settings from the Migration threshold drop-down menu.
9. In the **Host Options** section, configure the Lockdown mode, NTP server address, and host update preference.
   a) Select a lockdown mode from the drop-down menu.
   b) Optional: Enter an NTP server address or FQDN.

      If you enter more than one NTP server addresses, separate them by using commas.
   c) Optional: Select a host update option from the drop-down menu.

   The settings are applied across all hosts in this cluster.

10. Optional: In the **Enhanced vMotion Capability** section, enable EVC and select the CPU model from the EVC mode drop-down menu.
11. Click **Next**.

    The **Review** page appears.

12. Review the settings and select **Finish**.

    The card closes, and the progress of the operation appears in the **Recent Tasks** pane.

You have created a fully configured cluster in the vCenter Server inventory.

Expand your cluster by using the **Add hosts** card.

Extend a Cluster

You extend a configured cluster by adding hosts to it with the **Cluster quickstart** workflow in the vSphere Client.

After you configure your cluster, you can scale it out by adding more hosts. Then, you specify the network configuration for the new hosts in the cluster. During the initial configuration of the cluster, if you postponed configuring the host networking, no configuration, as for the existing hosts, is applied to the newly added hosts.

Extend a Cluster Without Host Networking Configuration

You extend a cluster by adding hosts to that cluster. If you previously configured the cluster without setting up the host networking, the configuration of the existing hosts in the cluster is applied to the new hosts.

- Verify that you have an existing cluster and hosts added to it.
- During the initial cluster configuration, select the Configure networking settings later check box. For more information, see Configure a Cluster.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- To add a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters** and select a configured cluster.
2. Right-click the cluster and select **Add Hosts**.

   The **Add hosts** wizard appears.

3. On the **Add hosts** page, add new or existing hosts to the cluster.
   - Add hosts that are not part of the vCenter Server inventory.
     a. Click the **New hosts** tab.
     b. Populate the IP Address and credentials text boxes for those hosts.
     c. To add more new hosts, click the **Add Host** button.
     d. To reuse the credentials for all added hosts, select the **Use the same credentials for all hosts** check box.
   - Add hosts that are managed by your vCenter Server instance and are in the same data center as your cluster.
     a. Click the **Existing hosts** tab.
     b. From the list, select the hosts that you want to add to the cluster.
4. Click **Next**.

   The **Host summary** page lists all hosts that will be added to the cluster and related warnings.

   Note: If a host cannot be validated automatically by the system, you are prompted to manually validate its certificate and accept its thumbprint in the **Security Alert** pop-up.
5. On the **Host summary** page, review the details of the added hosts and click **Next**.
6. Optional: On the **Import Image** page, select the host whose image to use as the image for the cluster.

   The **Import Image** page appears when you add hosts to a cluster managed with a single image. For information about adding a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.
7. On the **Ready to complete** page, click **Finish**.

   The **Extend Cluster Guide** page appears.
8. In the **Configure hosts** card, select **Configure**.

   A pop-up window appears. It informs you that the configuration for the hosts that exist in the cluster is applied to the newly added hosts.
9. Select **Continue**.

After successful validation, your newly added hosts are configured as the existing hosts in your cluster, and the **Configure** button in the **Configure hosts** card becomes inactive. You can only click **Re-validate** to verify the cluster configuration.

Configure the host networking manually and add more hosts to the cluster.

Use Quickstart to Extend a Cluster with Host Networking Configuration

You extend a hyper-converged cluster by adding hosts and configuring their networking to match the cluster configuration.

- Verify that you have an existing cluster and hosts added to it.
- In the initial cluster configuration, you configured the host networking.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.

- To add a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.

Note: If you modify any cluster networking settings outside of Quickstart, you cannot use the Quickstart workflow to add and configure new hosts to the cluster.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters** and select a configured cluster.
2. Right-click the cluster and select **Add Hosts**.
   The **Add hosts** wizard appears.
3. On the **Add hosts** page, add new or existing hosts to the cluster.
   - Add hosts that are not part of the vCenter Server inventory.
     a. Click the **New hosts** tab.
     b. Populate the IP Address and credentials text boxes for those hosts.
     c. To add more new hosts, click the **Add Host** button.
     d. To reuse the credentials for all added hosts, select the **Use the same credentials for all hosts** check box.
   - Add hosts that are managed by your vCenter Server instance and are in the same data center as your cluster.
     a. Click the **Existing hosts** tab.
     b. From the list, select the hosts that you want to add to the cluster.
4. Click **Next**.
   The **Host summary** page lists all hosts that will be added to the cluster and related warnings.

   Note: If a host cannot be validated automatically by the system, you are prompted to manually validate its certificate and accept its thumbprint in the **Security Alert** pop-up.
5. On the **Host summary** page, review the details of the added hosts and click **Next**.
6. Optional: On the **Import Image** page, select the host whose image to use as the image for the cluster.
   The **Import Image** page appears when you add hosts to a cluster managed with a single image. For information about adding a host to a cluster that you manage with a single image, see the *Managing Host and Cluster Lifecycle* documentation.
7. On the **Ready to complete** page, review the IP addresses or FQDN of the added hosts and click **Finish**.
   The **Extend Cluster Guide** page appears.
8. In the **Configure hosts** card, select **Configure**.
9. If the vSphere DRS feature is enabled on the cluster, configure the networking options in the **vMotion traffic** page.
   a) Optional: Select the **Use VLAN** check box and enter an ID for the vMotion distributed port group.
   b) Optional: Select a protocol type from the drop-down menu.
   c) Select an IP type from the drop-down menu.
   d) Optional: Populate the text boxes for each host in the cluster depending on the IP address type you need for setting up the networking.
      If the IP address type is set to `DHCP`, these text boxes are dimmed.
10. Click **Next**.
    The **Review** page appears.
11. Review the settings and select **Finish**.
    The card closes, and the progress of the operation appears in the **Recent Tasks** pane.

After successful validation, your newly added hosts are configured as the existing hosts in your cluster and the **Configure** button in the **Configure hosts** card becomes inactive. You can only click **Re-validate** to verify the cluster configuration.

Add more hosts to the cluster.

vSphere Tags and Attributes

Tags and attributes allow you to attach metadata to objects in the vSphere inventory to make it easier to sort and search for these objects.

A tag is a label that you can apply to objects in the vSphere inventory. When you create a tag, you assign that tag to a category. Categories allow you to group related tags together. When you define a category, you can specify the object types for its tags, and whether more than one tag in the category can be applied to an object.

For example, if you wanted to tag your virtual machines by guest operating system type, you can create a category called operating system. You can specify that it applies to virtual machines only and that only a single tag can be applied to a virtual machine at any time. The tags in this category might be Windows, Linux, and Mac OS.

Tags and categories can span multiple vCenter Server instances:

- If multiple on-premises vCenter Server instances are configured to use Enhanced Linked Mode, tags and tag categories are replicated across all these vCenter Server instances.
- When you use Hybrid Linked Mode, tags and tag categories are maintained across your linked domain. That means the on-premises SDDC and the VMware Cloud on AWS SDDC share tags and tag attributes.

For vSphere Tags and Attributes, VMware Cloud on AWS supports the same set of tasks as an on-premises SDDC.

Create, Edit, or Delete a Tag Category

You use categories to group tags together and define how tags can be applied to objects. You create, edit, and delete a tag category from the vSphere Client.

The required privilege depends on the task that you want to perform.

Task	Privilege
Create a tag category	**vSphere Tagging** > **Create vSphere Tag Category** on the root vCenter Server
Edit a tag category	**vSphere Tagging** > **Edit vSphere Tag Category** on the root vCenter Server.
Delete a tag category	**vSphere Tagging** > **Delete vSphere Tag Category** on the root vCenter Server.

You can create a tag category explicitly, as explained here, or as part of the tag creation process. Each tag has to belong to at least one tag category.

1. In the vSphere Client, click **Menu** > **Tags & Custom Attributes**.
2. Click the **Tags** tab and click **Categories**.
3. Start the task that you want to perform.

Option	Description
Create a tag category	Click the **New Category** icon.
Edit a tag category	Select a category and click the **Edit Category** icon.
Delete a tag category	Select a category from the list and click the **Delete Category** icon.

4. Edit the category options.

Option	Description
Category Name	The category name must be unique to the currently selected vCenter Server system.
Description	You can provide text in the description to describe the purpose or use of the category.
Tags Per Object	• If you select **One Tag**, you can apply only one tag from this category to an object. Use this option for categories whose tags are mutually exclusive. For example, if you have a category called Priority with tags High, Medium, and Low, then each object should have only one tag because an object can have only one priority. • If you select **Many tags**, you can apply more than one tag from the category to an object. Use this option for categories whose tags are not mutually exclusive. After you have set Tags Per Object, you can change from **One Tag** to **Many Tags**, but not from **Many Tags** to **One Tag**.
Associable Object Types	Select whether tags in this category can be assigned to all objects or only to a specific type of object, such as a virtual machine or a datastore. Changes to the associable object type are limited. • If you initially selected a single object type, you can later change the category to work for all object types. • If you initially selected All Objects, you cannot restrict the category later.

5. Click **OK** or **Yes** to confirm.

Create a Tag

You can use tags to add metadata to inventory objects. You can record information about your inventory objects in tags, and you can use the tags in searches.

For information about creating a tag category, see Create, Edit, or Delete a Tag Category.

1. In the vSphere Client, select **Menu** > **Tags & Custom Attributes**.
2. Select the **Tags** tab and click **Tags**.
3. Click **New**.
4. In the **Create Tag** dialog box, enter a name for the tag.
   You can use up to 256 characters for the name of the tag.
5. Enter a description of the tag.
6. Specify the tag category.
   - Select an existing category from the **Category** drop-down menu.
   - Click **Create New Category** and select the newly created category.
7. Click **Create**.

The tag appears in the list of tags.

Edit or Delete a Tag

In the vSphere Client, you can edit an existing tag or delete it when you no longer need it.

1. In the vSphere Client home, select **Menu** > **Tags & Custom Attributes**.
2. Select the **Tags** tab and click **Tags**.
3. Select a tag from the list.
4. Select your task.
   - To edit a tag, click **Edit** and confirm the operation.

     You can edit the name and description of the tag.
   - To delete a tag, click **Delete** and confirm the operation.

Assign or Remove a Tag

After you create tags, you can apply or remove them as metadata to objects in the vCenter Server inventory.

1. In the vSphere Client, navigate to an inventory tree.
2. Select an object from the list and click **Actions**.
3. From the drop-down menu, select **Tags and Custom Attributes**.
4. Select the required action.
   - To assign a tag, select **Assign Tag**.
   - To remove a tag, select **Remove tag**.
5. Select a tag from the list and confirm the operation.

   In the **Assign Tag** dialog box, you can also create new tags with the **Add tag** button. For information about creating a tag, see Create a Tag.

Add Permissions for Tags and Tag Categories

You can manage the user privileges for working with tags and categories. The procedure for assigning permissions to tags is the same as the procedure for assigning permissions to tag categories.

When you create a tag, you can specify which users and groups can operate with that tag. For example, you can grant administrative rights only to administrators and set read-only permissions for all other users or groups. You must have vSphere administrator credentials to set and manage permissions for tags.

Permissions for tags work similar to permissions for vCenter Server inventory objects. For more information, see the *vSphere Security* documentation.

1. In the vSphere Client, select **Menu** > **Tags & Custom Attributes**.
2. On the **Tags** tab, click the **Tags** or **Categories** button.

   Depending on the button that you click, you see the list of tags or the list of tag categories.

3. Select an item from the list and click **Add Permission**.
4. In the **Add Permission** dialog box, select a domain from the drop-down menu.
5. Search for a user or a group to add.
6. Select a role to add from the drop-down menu.
7. To enable permission inheritance, select the **Propagate to children** check box.
8. Click **OK**.

vSphere Tagging Best Practices

Incorrect tagging can lead to replication errors. To avoid these errors, diligently follow best practices when tagging objects in your vSphere environment.

When working with tags in multiple node situations, expect replication delays between the nodes (generally 30 seconds to 2 minutes depending on your setup).

Follow these best practices to avoid replication errors:

- After creating a tag, if you immediately assign that tag to a local object, assign it from the management node where you created the tag.
- After creating a tag, if you immediately assign that tag to a remote object, assign it from the management node to which the object is local. Depending on your environment setup, allow for replication time to propagate the new tag before you use the tag.
- Avoid simultaneously creating categories and tags from different management nodes before categories and tags across nodes can finish the replication process. If duplicate categories or tags are created from different nodes at the same time, the duplicates might not be detected and will appear. If you see these results, manually delete duplicates from one management node.
- Before you remove an object from the vCenter Server inventory that is not a virtual machine or a host, first remove the tags from the object.

For more information about tagging performance best practices, see the blog post titled *vSphere 7.0 U1 Tagging Performance Best Practices* at https://blogs.vmware.com/performance.

Custom Attributes

You can use custom attributes in the vSphere Client to assign user-specific values for each object of the custom attribute type.

After you create the attributes, set the value for the attribute on each virtual machine or managed host, as appropriate. This value is stored with vCenter Server and not with the virtual machine or managed host. Use the new attribute to filter information about your virtual machines and managed hosts. If you no longer need the custom attribute, remove it. A custom attribute is always a string.

For example, suppose that you have a set of products and you want to sort them by sales representative. Create a custom attribute for the sales person's name, Name. Add the custom attribute, Name, column to one of the list views. Add the appropriate name to each product entry. Click the column title Name to sort alphabetically.

The custom attributes feature is available only when you are connected to a vCenter Server system.

Add and Edit Custom Attributes

You can create custom attributes in the vSphere Client and associate the attribute with an object, such as a host, virtual machine, cluster, or network. You can also edit custom attributes.

After you create the attributes, set an appropriate value for the attribute on each virtual machine. This value is stored with vCenter Server and not with the virtual machine. Use the new attribute to filter your virtual machines. If you no longer need the custom attribute, remove it. A custom attribute is always a string.

For example, suppose that you have a set of products and you want to sort them by sales representative.

1. Create a Name custom attribute for the sales person's name.
2. Add the Name custom attribute column to one of the list views and add a name to each product entry.
3. You can now click the Name column to sort alphabetically by sales person.

Note: Tags and tag categories support a finer-grained mechanism for tagging your object. Consider using tags and tag categories instead of custom attributes.

1. In the vSphere Client Home menu, select **Tags and Custom Attributes**.
2. Click **Custom Attributes**.

   All currently defined custom attributes for vCenter Server are displayed.
3. Click **New**.
4. Enter the values for the custom attribute.
   a) Type the name of the attributes in the **Attribute** text box.
   b) Select the attribute type from the **Type** drop-down menu.
   c) Click **OK**.

   After you have defined an attribute on an object, it is available to all objects of that type in the inventory. However, the value you specify is applied only to the currently selected object.
5. You can later edit a custom attribute.
   a) Select the attribute and click **Edit**.
   b) Change the Name.
   c) Change the type if it's available.
   d) Click **OK**.

Working with Tasks

vSphere tasks are activities and actions that occur on an object within the vSphere inventory.

View Tasks

Tasks represent system activities that do not complete immediately, such as migrating a virtual machine. For example, powering off a virtual machine is a task. You can perform this task manually every evening, or you can set up a scheduled task to power off the virtual machine every evening.

You can view tasks that are associated with a single object or all objects in a vSphere environment. By default, the task list for an object also includes tasks performed on its child objects. You can filter the task list by entering the object that you want in the **Target** column filter.

If you are logged in to a vCenter Server instance that is part of a vCenter Enhanced Linked Mode group, the **Server** column in the task list displays the name of the vCenter Server system on which the task is performed.

1. In the vSphere Client, navigate to an object in the inventory.
2. Click the **Monitor** tab.
3. Under **Tasks and Events**, select **Tasks**.

   The task list contains tasks performed on the object and detailed information, such as target, task status, initiator, and start/completion time of the task.

   You can limit the number of tasks visible in the **Tasks** pane by selecting an option from the**Items per page** drop-down menu.
4. Optional: Click the filter ( ) icon on a column header and filter the task list by entering your filtering criteria.
5. Optional: Click the expand row ( ) icon to view related events for a task. You can view task information about multiple tasks at the same time.

How Do You Cancel a vSphere Task

Canceling a vSphere task stops a running task from occurring. Canceling a scheduled task does not cancel subsequent runs. To cancel a scheduled task that has not run, reschedule it.

Required privileges:

- Manual tasks: **Tasks** > **Update task**
- Scheduled tasks:**Scheduled task** > **Remove task**

1. Locate the task in the **Recent Tasks** pane.

   By default, the **Recent Tasks** pane is displayed at the bottom of the vSphere Client.
2. Click the cancel button ( ) next to the progress bar in the Status column for the task you want.

   If the cancel option is unavailable, the selected task cannot be canceled.
3. In the **Cancel Task** pop-up dialog box, click **OK**.

The vCenter Server system or ESXi host stops the progress of the task and returns the object to its previous state. The vSphere Client displays the task with a *The task was canceled by a user.* status.

Cancelled tasks and the corresponding events are retained in the vCenter Server database. For information about the retention of tasks and events in the vCenter Server database, and how to configure the database settings, see the *vSphere Monitoring and Performance* documentation.

Export Tasks

You can export the detailed information for selected tasks or all tasks listed in the **Tasks** page to a CSV file.

To export the information about specific tasks, you can filter the task list and then select only the tasks that you want. You can also export the information about all tasks listed for an object or all objects in the vSphere environment.

1. In the vSphere Client, navigate to an object in the inventory.
2. Click the **Monitor** tab.
3. Under **Tasks and Events**, select **Tasks**.
4. Optional: To export one or more tasks, click the check boxes in front of the respective tasks.
5. Click the **EXPORT** option at the bottom left corner of the **Tasks** pane.

   Note: By default, if you did not select any tasks, the detailed information about all displayed tasks is exported.

   a) Optional: If you selected one or more tasks but you want to export the information about all displayed tasks, click **All Rows**.
   b) Optional: If you want to export only the information for the selected tasks, click **Selected Rows**.

   The CSV file is generated and available for download.

Schedule Tasks

You can schedule tasks to run once in the future or multiple times, at a recurring interval.

The tasks you can schedule are listed in the following table.

Table 144: Scheduled Tasks

Scheduled Task	Description
Add a host	Adds the host to the specified data center or cluster.
Change the power state of a virtual machine	Powers on, powers off, suspends, or resets the state of the virtual machine.
Change cluster power settings	Activate or deactivate DPM for hosts in a cluster.
Change resource settings of a resource pool or virtual machine	Changes the following resource settings: • CPU – Shares, Reservation, Limit. • Memory – Shares, Reservation, Limit.
Check compliance of a profile	Checks that a host's configuration matches the configuration specified in a host profile.
Clone a virtual machine	Makes a clone of the virtual machine and places it on the specified host or cluster.
Create a virtual machine	Creates a new virtual machine on the specified host.
Deploy a virtual machine	Creates a new virtual machine from a template on the specified host or cluster.
Migrate a virtual machine	Migrate a virtual machine to the specified host or datastore by using migration or migration with vMotion.
Make a snapshot of a virtual machine	Captures the entire state of the virtual machine at the time the snapshot is taken.
Scan for Updates	Scans templates, virtual machines, and hosts for available updates. This task is available only when is installed.
Remediate	Installs missing patches from the baselines selected for remediation on the hosts discovered during the scan operation and applies the newly configured settings. This task is available only when is installed.

You create scheduled tasks by using the **Scheduled Task** wizard. For some scheduled tasks, this wizard opens the wizard used specifically for that task. For example, if you create a scheduled task that migrates a virtual machine, the **Scheduled Task** wizard opens the **Migrate Virtual Machine** wizard, which you use to set up the migration details.

Scheduling one task to run on multiple objects is not possible. For example, you cannot create one scheduled task on a host that powers on all virtual machines on that host. You must create a separate scheduled task for each virtual machine.

After a scheduled task runs, you can reschedule it to run again at another time.

Create a Scheduled Task

You can create scheduled tasks for operations that you want to run automatically once or at a recurring interval.

Required privilege: **Schedule Task** > **Create tasks**

If the task to schedule is not available in the vSphere Client, use the vSphere API. See the *vSphere SDK Programming Guide*.

CAUTION: Do not schedule multiple tasks simultaneously on the same object. The results are unpredictable.

1. In the vSphere Client, navigate to the object for which you want to schedule a task.
2. Select **Configure** > **Scheduled Tasks** > **New Scheduled Task**.
3. From the **New Scheduled Task** drop-down menu, select the task to schedule.

   The **Schedule New Task** wizard opens for the task with the task name appended next to the name of the wizard. The wizard contains a page where you configure the scheduling options for the task.
4. Enter the required scheduling options for the task.
   a) Enter a name and description of the task.
   b) Choose a frequency for the task.

Option	Description
Once	Runs the scheduled task at the time selected.
After vCenter startup	Runs the task a specified number of minutes after vCenter Server startup.
Hourly	1. Enter the repeat frequency. 2. Enter the start date and time. 3. Enter the end date and time. For example, to start a task at the half-hour mark of every fifth hour, enter `5` hours and `30` minutes.
Daily	1. Enter the repeat frequency. 2. Enter the start date and time. 3. Enter the end date and time. For example, to run the task at 2:30 pm every four days, enter `4` and `14:30`.
Weekly	1. Enter the repeat frequency. 2. Select the day of the week. 3. Enter the start date and time. 4. Enter the end date and time. For example, to run the task at 6 am every Tuesday and Thursday, enter **1** week, **6 am**, and select **Tuesday** and **Thursday**.
Monthly	1. Enter the repeat frequency.

Option	Description
	2. Select the days by using one of the following methods. – Enter a specific day of the month and the number of months. For example, the tenth day every five months. – Select **first**, **second**, **third**, **fourth**, or **last**, and select the day of the week and the number of months. **last** runs the task on the last week in the month that the day occurs. For example, if you select the last Monday of the month and the month ends on a Sunday, the task runs six days before the end of the month.

c) Optional: Enter one or more email addresses to receive an email notification when the task is complete.

To schedule some tasks, you must enter additional details for the task. For example, to schedule taking a virtual machine snapshot, the **Schedule New Task (Take Snapshot)** wizard opens. In the **Scheduling Options** page, you set the scheduling options for the task, and in the **Snapshot Settings** page, you enter the properties for the snapshot.

5. Click **Finish**.

Change or Reschedule a Task

After a scheduled task is created, you can change the schedule, frequency, and other attributes of the task. You can edit and reschedule tasks before or after they run.

Required privilege:**Schedule Task** > **Modify**

1. In the vSphere Client, navigate to the object for which you want to edit a scheduled task.
   To view all scheduled tasks for a vCenter Server instance, navigate to that vCenter Server instance.
2. Select **Configure**, and select **Scheduled Tasks**.
3. Select a task from the list on the left and click **Edit**.
4. Right-click the task and select **Edit**.
5. Change the task attributes as necessary.
6. Click **Save**.

Remove a Scheduled Task

Removing a scheduled task removes all future occurrences of the task. The history associated with all completed occurrences of the task remains in the vCenter Server database.

Required privilege:**Scheduled task** > **Remove**

1. In the vSphere Client, navigate to the object for which you want to remove a scheduled task.
   To view all scheduled tasks for a vCenter Server instance, navigate to that vCenter Server instance.
2. Select **Configure**, and select **Scheduled Tasks**.
3. Select a task from the list on the left and click **Remove**.

Configuring Hosts in vCenter Server

Before you set up your virtual environment and consider how the virtual machines that it will support are going to be used and administered, you should configure ESXi hosts in vCenter Server. The configuration of ESXi hosts involves several tasks.

Host Configuration

Before you create virtual machines on your hosts, you must configure the hosts to ensure that they have correct licensing, network and storage access, and security settings.

For information on configuring a host, see the configuration information for the specific vSphere component in the *vSphere Security*documentation, the *vSphere Storage* documentation, and the *vSphere Networking* documentation.

Configure the Boot Device on an ESXi Host

On servers running ESXi, you can select the device that the server boots from.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a host in the inventory and click the **Configure** tab.
3. Under Hardware, select **Overview** and click the **Boot Options** button.
4. Select a boot device from the drop-down menu.
5. Optional: To reboot immediately from the device you selected, select **Apply and Reboot on OK**.
   If you do not select **Apply and Reboot on OK**, the new setting takes effect when the host reboots next.
6. Click **OK**.

Configure Agent VM Settings

You can configure the datastore and network settings for the ESX agent virtual machines that you deploy on a host.

An ESX agent is a virtual machine, or a virtual machine and a vSphere Installation Bundle (VIB), that extend the functions of an ESXi host to provide additional services that a vSphere solution requires.

For example, a solution might require a particular network filter or firewall configuration to function. A solution can use an ESX agent to connect to the vSphere Hypervisor and extend the host with functions specific to that solution. For example, the ESX agent can filter network traffic, act as a firewall, or gather other information about the virtual machines on the host.

When you configure the datastore and network settings for ESX agents on a host, all of the ESX agents that you deploy on the host use that datastore and network configuration.

Important: ESX agents are deployed only if you configure the network and datastore settings.

1. Select a host in the vSphere Client inventory.
2. Click the **Configure** tab.
3. Under **Virtual Machines**, select **Agent VM Settings**.
   The current settings for the ESX agents on the host, if any, appear.
4. Click **Edit**.
5. From the **Datastore** drop-down menu, select a datastore in which to deploy the ESX agent virtual machines.
6. From the **Network** drop-down menu, select a network to connect the ESX agents.
7. Click **OK**.

For information about ESX agents and ESX Agent Manager, see *Developing and Deploying vSphere Solutions, vServices, and ESX Agents*.

Set Advanced Host Attributes

You can set advanced attributes for a host.

CAUTION: Changing advanced options is considered unsupported. Typically, the default settings produce the optimum result. Change the advanced options only when you get specific instructions from VMware technical support or a knowledge base article.

1. Browse to the host in the vSphere Client.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. Click the **Edit** button.
5. Find the appropriate item and change the value.
6. Click **OK**.

Synchronizing Clocks on the vSphere Network

Verify that all components on the vSphere network have their clocks synchronized. If the clocks on the physical machines in your vSphere network are not synchronized, SSL certificates and SAML tokens, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server`vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause the first boot of a component in your environment to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server is not synchronized with NTP or PTP. Similarly, issues can arise if the destination vCenter Server migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server instance.

- The target ESXi host where the destination vCenter Server is to be deployed is synchronized to NTP or PTP.
- The ESXi host running the source vCenter Server is synchronized to NTP or PTP.
- When upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, if the vCenter Server appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP or PTP.
- If you are upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, verify that the source vCenter Server or vCenter Server appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the VMware knowledge base article at https://kb.vmware.com/s/article/1318.

To synchronize ESXi clocks with an NTP or a PTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see topic *Edit the Time Configuration of an ESXi Host in the VMware Host Client* in the *vSphere Single Host Management - VMware Host Client* documentation.

To learn how to change time synchronization settings for vCenter Server, see topic *Configure the System Time Zone and Time Synchronization Settings* in the *vCenter Server Configuration* documentation.

To learn how to edit the time configuration for a host by using the vSphere Client, see topic *Editing the Time Configuration Settings of a Host* in the *vCenter Server and Host Management* documentation.

Editing the Time Configuration Settings of a Host

To ensure precise timestamping of events and synchronization of the time between an ESXi host and the other components in the vSphere network, configure the time settings of the ESXi host manually or synchronize the time and date of the host with an NTP or PTP server.

Exact timestamping shows the precise sequence of events that occur in the vSphere network. Time synchronization between the components of the vSphere network can prevent authentication problems, backup issues, and incorrect logs.

To ensure that all components in your environment have the correct time, as a best practice you must use the same time synchronization mechanism across the board.

Configure the Date and Time on a Host Manually

You can configure the date and time of the ESXi host manually. You can use the manual time configuration only after you stop synchronizing the time and date with NTP or PTP.

- Verify that the NTP and the PTP configurations are not used on the host.

If you notice some significant clock skew between a host in your environment and the rest of the vSphere components, you might need to first manually set the time and date on the host before synchronizing it to an NTP server or PTP.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a host.
3. On the **Configure** tab, select **System** > **Time Configuration**.
4. Click **Manual Set-Up**.

   The **Manual time configuration** dialog box appears.
5. Enter a date and time and click **OK**.

   Note:

   ESXi hosts use UTC (Coordinated Universal Time) and do not support changing time zones. In the vSphere Client, you see your local time as the current host time.

Use NTP Servers for Time and Date Synchronization of a Host

To avoid time synchronization problems between an ESXi host and other components in the vSphere network, you can synchronize the time and date of the host to an NTP server.

- Verify that the PTP service is not running. For information about how to change its status, see Manage the NTP and PTP Service Status on the Host.

The NTP and the PTP services cannot run simultaneously. Deactivate the PTP service and then activate the NTP server synchronization. Additionally, when you activate the NTP service, the manual time configuration becomes inactive.

Note:

You can set a startup policy to control the start and stop of the NTP service. You can also change the NTP service status manually. For more information about services, see Manage the NTP and PTP Service Status on the Host.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a host.
3. On the **Configure** tab, select **System** > **Time Configuration**.
4. Click **Add Service** and select **Network Time Protocol** from the drop-down menu.
5. In the **Network Time Protocol** dialog box, edit the network time protocol settings.
   a) To monitor all events in the vSphere environment, select **Enable monitoring events**.
   b) In the **NTP Servers** text box, enter the IP addresses or host names of the NTP servers that you want to use. A best practice is to use at least three NTP servers for the time synchronization of the host.
   c) Click **OK**.

   The NTP configuration is triggered immediately.

Use PTP for Time and Date Synchronization of a Host

To ensure that the time of an ESXi host is synchronized with the time of other components of the vSphere network, you can synchronize the time and date of the host to PTP.

- Verify that the NTP service is not running. For information about how to change its status, see Manage the NTP and PTP Service Status on the Host.
- For a hardware-based timestamping, verify that you enabled PCI passthrough for a network device on the host. See the *vSphere Networking* documentation.

The Precision Time Protocol allows both software- and hardware-based timestamping on an ESXi hosts and provides a highly accurate time synchronization. Starting with vSphere 7.0 Update 3, PTP provisions hardware-based timestamping for the virtual machines and the hosts within a network.

The PTP and the NTP services cannot run simultaneously. Stop the NTP service and then enable the PTP service. Additionally, when you enable the PTP service, the manual time configuration becomes inactive.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a host.
3. On the **Configure** tab, select **System** > **Time Configuration**.
4. Click **Add Service** and select **Precision Time Protocol** from the drop-down menu.
5. In the **Precision Time Protocol** dialog box, edit the PTP settings.
   a) Select the PTP-enabled network device for time synchronization from the **Network adapter type** drop-down menu.

PCI passthrough	For configuring a hardware timestamping with a PCI passthrough network device, follow these steps: 1. From the **Device name** drop-down menu, select the PCI passthrough network device. For vSphere 7.0 U3, the supported network adapters are IntelX710 and E810. 2. Enter the IP configuration settings for the network device. – To use DHCP to obtain the IP address configuration of the network device, select **Obtain IPv4 settings automatically**. – To set a static IP configuration, select the **Use static IPv4 settings** option and enter the IPv4 configuration settings. – To use the IEEE 802.3 network transport, select **No IP configuration (use IEEE 802.3 transport)**.

VMkernel Adapter	For configuring software timestamping PTP, from the **Device name** drop-down menu, select the VMkernel adapter configured to use PTP.

6. Optional: Create a fallback mechanism in case the PTP synchronization fails.
   a) To monitor the events in vSphere, select the **Enable monitoring events** check box.
   b) To enable a fallback mechanism in case PTP become inaccessible, click **Enable fallback**.

      You can create a fallback mechanism only if you enabled tracking the events in vSphere.
   c) In the **NTP Servers** text box, enter the IP addresses or host names of the NTP servers that you want to use. A best practice is to use at least three NTP servers for the time synchronization of the host.
7. Click **OK**.

   Finishing the configuration immediately triggers the PTP synchronization.
8. Optional: To test whether the service used for time synchronization of the host is running correctly, click **Test Services**.

   The **Time Synchronization Services test** dialog box appears. You can see information about how the activated time configuration works by collecting information from various systems.

Manage the NTP and PTP Service Status on the Host

You can configure a startup policy for the NTP or PTP service that runs on the host. You can also manually start, stop, or restart the respective service and in this way override the configured startup policy.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a host.
3. On the **Configure** tab, select **System** > **Services**.
4. Change the status of the NTP or PTP service manually.

Option	**Description**
Option	Action
Change the NTP service status	1. Select **NTP Daemon**. 2. Click **Start**, **Stop**, or **Restart**.
Change the PTP service status	1. Select **PTP Daemon**. 2. Click **Start**, **Stop**, or **Restart**.

5. Optional: Select the NTP or PTP service and click **Edit Startup Policy**.

Option	**Description**
Start and stop with port usage	Starts or stops the service when a client port is activated or deactivated for access to the security profile of the host.
Start and stop with host	Starts and stops the service when the host powers on and shuts down.
Start and stop manually	You must manually control the status of the service.

Delete a Time Synchronization Service on a Host

Delete a time synchronization service that is no longer needed.

Verify that the service you want to delete is not used to synchronize the time of the host.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. Select a host.
3. On the **Configure** tab, select **System** > **Time Configuration**.
4. Select the **Precision Time Protocol** or **Network Time Protocol** check box and click **Delete**.
5. Click **OK**.

Managing Hosts in vCenter Server

To monitor all hosts in your virtual environment from one place and to simplify host configuration, connect the hosts to a vCenter Server system.

For information about configuration management of ESXi hosts, see the *vSphere Networking* documentation, the *vSphere Storage* documentation, and the *vSphere Security* documentation.

Disconnecting and Reconnecting an ESXi Host

You can disconnect and reconnect a host that a vCenter Server system manages. Disconnecting a managed host does not remove it from vCenter Server, but temporarily suspends all monitoring activities that vCenter Server performs.

The managed host and its associated virtual machines remain in the vCenter Server inventory. By contrast, removing a managed host from vCenter Server deletes the managed host and all its associated virtual machines from the vCenter Server inventory.

If an ESXi host becomes disconnected due to a loss of network connectivity to vCenter Server, the ESXi host reconnects automatically to vCenter Server after network connectivity is restored. If you manually disconnect an ESXi host, see Reconnect a Managed Host for more information.

Reconnecting an ESXi host automatically or manually does not impact the running virtual machines, unless the host is part of a cluster and there are resource pool privileges configured. For more information about creating and managing resource pools, see the *vSphere Resource Management* documentation.

Tip:

You can use the API to automate the management of managed ESXi hosts. For more information about the available options, see the *vCenter Host APIs* reference documentation.

Disconnect a Managed Host

Use the vSphere Client to disconnect a managed host from vCenter Server.

1. Navigate to **Home** > **Hosts and Clusters** and select a host.
2. Right-click the host and select **Connection** > **Disconnect** from the pop-up menu.
3. In the confirmation dialog box that appears, click **Ok**.

   If the managed host is disconnected, the word “disconnected” is appended to the object name in parentheses, and the object is dimmed. All associated virtual machines are similarly dimmed and labeled.

Reconnect a Managed Host

Use the vSphere Client to reconnect a managed host to a vCenter Server system.

1. Navigate to **Home** > **Hosts and Clusters** and select a host.
2. Right-click the host and select **Connection** > **Connect** from the pop-up menu.

   When the managed host's connection status to vCenter Server is changed, the statuses of the virtual machines on that managed host are updated to reflect the change.

Reconnecting Hosts After Changes to the vCenter Server SSL Certificate

vCenter Server uses an SSL certificate to encrypt and decrypt host passwords stored in the vCenter Server database. If the certificate is replaced or changed, vCenter Servercannot decrypt host passwords, and therefore cannot connect to managed hosts. If vCenter Server fails to decrypt a host password, the host is disconnected from vCenter Server.

You must reconnect the host and supply the login credentials, which are encrypted and stored in the database using the new certificate.

Relocate a Host

You can move a host to another location within the vSphere inventory by dragging the host to the new location. The new location can be a folder, a cluster, or you can place the host as a standalone object in the data center.

Power off all virtual machines that are running on the host, or migrate the virtual machines to a new host by using vMotion.

When a host is moved from a cluster to another destination in the vSphere inventory, the resources which the host provides are deducted from the total cluster resources. You can either keep the virtual machines in the same cluster and migrate them to other hosts, or keep them on the host and remove them from the cluster. For information about removing a host from a cluster, see the *vSphere Resource Management* documentation.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters** and select a host.
2. If the host is part of a cluster, put it in maintenance mode.
   a) Right-click the host and select **Maintenance Mode** > **Enter Maintenance Mode**.
   b) Optional: If the host is part of a DRS cluster, evacuate the powered off or suspended virtual machines to other hosts within the cluster by selecting the check box **Move powered-off and suspended virtual machines to other hosts in the cluster**.
   c) In the confirmation dialog box, click **OK**.

      The host enters maintenance mode.
3. Select the host in the vSphere inventory panel and drag it to the new location within the inventory.
4. Right-click the host and select **Maintenance Mode** > **Exit Maintenance Mode**.
5. Optional: Power on the virtual machines that you powered off before you put the host in maintenance mode.

Remove a Host from vCenter Server

Remove a managed host from vCenter Server to stop vCenter Server from monitoring and managing that host.

- Make sure that NFS mounts are active. If NFS mounts are unresponsive, the operation fails.

- If the host you want to remove from the cluster is connected to a distributed switch, remove the host from the switch. For more information, see Remove Hosts from a vSphere Distributed Switch in the *vSphere Networking*documentation.

If possible, remove managed hosts while they are connected. Removing a disconnected host does not remove the vCenter Server agent from the managed host.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. 2. Select a host in the inventory.
3. Optional: If the host is part of a cluster, put it in maintenance mode.
   a) Right-click the host and select **Maintenance Mode** > **Enter Maintenance Mode** from the pop-up menu.

      If not all virtual machines on the host are powered off, the host does not enter maintenance mode.

      If the host is part of a DRS cluster, when the host enters maintenance mode, DRS attempts to evacuate powered on virtual machines from the host by using vMotion.
   b) In the confirmation dialog box, click **Ok**.

      If the host is part of a DRS cluster, you can evacuate powered off or suspended virtual machines to other hosts within the cluster. Select the check box **Move powered-off and suspended virtual machines to other hosts in the cluster**.

      The host icon changes and the term Maintenance Mode is added to the name in parentheses.
4. Right-click the host you want to remove in the inventory pane, and select **Remove from Inventory** from the pop-up menu.
5. In the confirmation dialog box, click **Yes** to remove the host.

   vCenter Server removes the host and the associated virtual machines from the vCenter Server instance. vCenter Server then returns the status of all associated processor and migration licenses to available.

Reboot or Shut Down an ESXi Host

You can power off or restart any ESXi host using the vSphere Client. Powering off a managed host disconnects it from vCenter Server, but does not remove it from the inventory.

- Power off all virtual machines that are running on the host, or migrate the virtual machines to a new host by using vMotion.
- Put the host in maintenance mode.

To shut down or reboot an ESXi host, you can use the ESXCLI command set. See the *Stopping and Rebooting Hosts with ESXCLI* topic in the *ESXCLI Concepts and Examples* documentation at https://developer.broadcom.com.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters** and select a host.
2. From the **Actions** menu, select **Power**.
3. Select the operation.
   - To power off and restart the ESXi host, click **Reboot**.
   - To power off the ESXi host, click **Shut Down**.
4. Provide a reason for the operation and click **OK**.

   This information is added to the log file.

Verifying SSL Certificates for Legacy Hosts

You can configure vCenter Server to check the SSL certificates of hosts to which it connects. If you configure this setting, vCenter Server and the vSphere Client check for valid SSL certificates before connecting to a host for operations such as adding a host or making a remote console connection to a virtual machine.

vCenter Server 5.1 and vCenter Server 5.5 always connect to ESXi hosts using SSL thumbprint certificates. Starting with vCenter Server 6.0, the SSL certificates are signed by VMware Certificate Authority by default. You can instead use certificates from a third-party CA. Thumbprint mode is supported only for legacy hosts.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. Select **SSL settings**.
6. Determine the host thumbprint for each legacy host that requires validation.
   a) Log in to the direct console.
   b) Select **View Support Information** on the **System Customization** menu.
      The thumbprint is displayed in the column on the right.
7. Compare the thumbprint you obtained from the host with the thumbprint listed in the vCenter Server SSL settings dialog box.
8. If the thumbprints match, select the check box for the host.
   Hosts that are not selected will be disconnected after you click **Save**.
9. Click **Save**.

License and Subscription Management

vSphere provides a centralized license management system that you can use to manage licenses for ESXi hosts, vCenter Server systems, vSAN clusters, Supervisor Clusters, and solutions. To leverage several cloud capabilities while you manage your on-premises vSphere infrastructure, you can convert your vCenter Servers and vSAN clusters to subscription.

For more information about how to get access to cloud services for your on-premises vSphere environments, see the *VMware vSphere+* documentation.

Licensing and Subscription Terminology and Definitions

The licensing system in vSphere uses specific terminology and definitions to refer to different licensing-related objects.

License Key	A license key encodes details about the product it is associated with, the license expiration date, the license capacity, and other information. The license key is assigned to an object to activate the functionality of its associated product.
License	A container for a license key of a VMware product. To use a license key, you create a license object in the vSphere Client and insert the license key into the license. After the license is created, you can assign it to assets.
Product Edition	A set of specific features that are associated with a unique license key. When assigned, the license key unlocks the features in the product edition. Examples of product editions are vSphere

	Enterprise Plus, vSphere Standard, vCenter Server Essentials, and so on.
Feature	Activated or deactivated functionality by a license that is associated with a specific product edition. Examples of features are vSphere DRS, vSphere vMotion, and vSphere High Availability.
Solution	A product that is packed and distributed independently from vSphere. You install a solution in vSphere to take advantage of certain functionality. Every solution has a licensing model specific for the solution, but uses the License Service for license management and reporting. Examples of solutions are VMware Site Recovery Manager, vRealize Operations Manager, vCloud Network and Security, and so on.
Asset	Any object in vSphere that requires licensing. If the license has sufficient capacity, the license administrator in vSphere can assign one license to one or multiple assets of the same type. Suite licenses can be assigned to all assets that are part of the suite. Assets are vCenter Server systems, ESXi hosts, and products that integrate with vSphere such as VMware Site Recovery Manager, vRealize Operations Manager, and others.
License Capacity	The number of units that you can assign to assets. The units of a license capacity can be of different types depending on the product that the license is associated with. For example, a license for vCenter Server determines the number of vCenter Server systems that you can license.
License Use	The number of units that an asset uses from the capacity of a license. For example, if you assign a per-virtual-machine license to VMware Site Recovery Manager, the license use for VMware Site Recovery Manager is the number of protected virtual machines.
Subscription Capacity	The number of cores required per CPU for a single ESXi host that you must purchase when you are ready to convert to a vSphere+ and vSAN+ subscription.
Free Trial	A 60-day period of time during which you can explore all the vSphere+ and vSAN+capabilities offered for your on-premises vCenter Server instances with the exception of the upgrade functionality from the VMC Console.

The License Service in vSphere 7.0

In vSphere 7.0, the License Service is part of the vSphere environment. The License Service delivers centralized license management and reporting functionality to vSphere and to products that integrate with vSphere.

You can use the License Service with newly installed vSphere 6.0 and later environments. You can also use the License Service with environments that are upgraded from vSphere 5.x to vSphere 6.0 and later. For details about upgrading the license management in vCenter Server 5.x to the License Service in vSphere 6.0 and later, see the *vSphere Upgrade* guide.

The License Service provides an inventory of licenses in the vSphere environment, and manages the license assignments for ESXi hosts, vCenter Server systems, vSAN clusters, and Supervisor Clusters. The License Service also manages the license assignments for products that integrate with vSphere, such as vRealize Operations Manager, and VMware Site Recovery Manager.

If your vSphere environment has several vCenter Server systems that are joined in Enhanced Linked Mode, the licensing inventory is replicated across all linked vCenter Server systems. This way, the licensing data for each asset and all

available licenses are replicated across all linked vCenter Server systems. Each individual vCenter Server system contains a copy of that data and licenses for all linked vCenter Server systems.

Note: Licensing data is replicated across multiple linked vCenter Server systems on a 10-minute interval.

For example, suppose that your environment consists of eight vCenter Server systems that are joined in Enhanced Linked Mode, and every vCenter Server system has 10 hosts connected to it. The License Service stores information about the license assignments and uses for all eight vCenter Server systems, and the 80 hosts that are connected to those systems. With the License Service, you can manage the licensing for all eight vCenter Server systems and the 80 hosts that are connected to them through the vSphere Client.

Licensing for Environments with vCenter Server Systems 6.0 and Later, and 5.5

If your vSphere 6.0 or later environment consists of vCenter Server 6.0 or later, and 5.5 systems, consider the differences in the license management and reporting between vSphere 6.0 and later, and vSphere 5.5.

The License Service in vSphere 6.0 and later manages the licensing data for all ESXi hosts, vSAN clusters, and solutions that are associated with the vCenter Server 6.0 and later systems in the vSphere environment. However, every standalone vCenter Server 5.5 system manages the licensing data only for the hosts, solutions, and vSAN clusters that are associated with that system. Licensing data for linked vCenter Server 5.5 systems is replicated only for the vCenter Server 5.5 systems in the group.

Due to the architectural changes in vSphere 6.0 and later, you can either manage the licensing data for all assets that are associated with all vCenter Server 6.0 and later systems in vSphere, or manage the licensing data for individual vCenter Server 5.5 systems or a group of linked vCenter Server 5.5 systems. The licensing interface in the vSphere Client allows you to select between all vCenter Server 6.0 and later systems and vCenter Server 5.5 systems.

Licensing and Subscription for Products in vSphere

ESXi hosts, vCenter Server, vSAN clusters, and Supervisor Clusters are licensed differently. To apply their licensing models correctly, you must understand how the associated assets consume the license capacity. You can also convert your on-premises vSphere infrastructure to subscription by purchasing vSphere+ and vSAN+ subscriptions.

Licensing for ESXi Hosts

ESXi hosts are licensed with vSphere licenses. Each vSphere license has a certain capacity that you can use to license multiple physical CPUs on ESXi hosts.

Starting with vSphere 7.0, one CPU license covers one CPU with up to 32 cores. If a CPU has more than 32 cores, you need additional CPU licenses.

Number of CPUs	Cores per CPU	Number of CPU Licenses
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

When you assign a vSphere license to a host, the amount of capacity consumed is determined by the number of physical CPUs on the host and the number of physical cores in each physical CPU.

vSphere Desktop that is intended for VDI environments is licensed on per virtual machine basis.

To license an ESXi host, you must assign it a vSphere license that meets the following prerequisites:

- The license must have sufficient capacity to license all physical CPUs on the host.

- The license must support all the features that the host uses. For example, if the host is associated with a vSphere Distributed Switch, the license that you assign must support the vSphere Distributed Switch feature.

If you attempt to assign a license that has insufficient capacity or does not support the features that the host uses, the license assignment fails.

If you use the licensing model with up to 32 cores, you can assign a vSphere license for 10 32-core CPUs to any of the following combinations of hosts:

- Five 2-CPU hosts with 32 cores per CPU
- Five 1-CPU hosts with 64 cores per CPU
- Two 2-CPU hosts with 48 cores per CPU and two 1-CPU hosts with 20 cores per CPU

Dual-core and quad-core CPUs, such as Intel CPUs that combine two or four independent CPUs on a single chip, count as one CPU.

Evaluation Mode

After you install ESXi, it operates in evaluation mode for up to 60 consecutive days. An evaluation mode license provides all features of the highest vSphere product edition.

After you assign a license to an ESXi host, at any time before the evaluation period expires, you can set the host back to evaluation mode to explore the entire set of features available for the remaining evaluation period.

For example, if you use an ESXi host in evaluation mode for 20 days, then assign a vSphere Standard license to the host, and 5 days later set the host back to evaluation mode, you can explore the entire set of features available for the host for the remaining 35 days of the evaluation period.

License and Evaluation Period Expiry

For ESXi hosts, license or evaluation period expiry leads to disconnection from vCenter Server. All powered on virtual machines continue to work, but you cannot power on virtual machines after they are powered off. You cannot change the current configuration of the features that are in use. You cannot use the features that remained unused before the license expiration.

Note: When there are expiring licenses, a notification appears 90 days before the license expiration.

Licensing ESXi Hosts After Upgrade

If you upgrade an ESXi host to a version that starts with the same number, you do not need to replace the existing license with a new one. For example, if you upgrade a host from ESXi 5.1 to 5.5, you can use the same license for the host.

If you upgrade an ESXi host to a major version that starts with a different number, the evaluation period restarts and you must assign a new license. For example, if you upgrade an ESXi host from 5.x to 6.x, you must license the host with a vSphere 6 license.

vSphere Desktop

vSphere Desktop is intended for VDI environments such as Horizon View. The license use for vSphere Desktop equals the total number of powered on desktop virtual machines running on the hosts that are assigned a vSphere Desktop license.

Licensing for vCenter Server

vCenter Server systems are licensed with vCenter Server licenses that have per-instance capacity.

To license a vCenter Server system, you need a vCenter Server license that has the capacity for at least one instance.

Evaluation Mode

When you install a vCenter Server system, it is in evaluation mode. An evaluation mode license of a vCenter Server system expires 60 days after the product is installed no matter whether you assign a license to vCenter Server or not. You can set vCenter Server back to evaluation mode only within 60 days after its installation.

For example, suppose that you install a vCenter Server system and use it in evaluation mode for 20 days and assign the system an appropriate license. The evaluation mode license of vCenter Server expires after the remaining 40 days of the evaluation period.

License and Evaluation Period Expiry

When the license or evaluation period of a vCenter Server system expires, all hosts disconnect from that vCenter Server system. The virtual machines running on the disconnected hosts remain intact. Until the vCenter Server system is assigned a new license, you can manage the virtual machines on the disconnected hosts by logging into each host separately. After vCenter Server is assigned to a new license key, all disconnected hosts reconnect to the vCenter Server system.

Note: When there are expiring licenses, a notification appears 90 days before the license expiration.

Licensing vCenter Server After Upgrade

If you upgrade vCenter Server to a version that starts with the same number, you can keep the same license. For example, if you upgrade a vCenter Server system from vCenter Server 5.1 to 5.5., you can keep the same license on the system.

If you upgrade vCenter Server to a major version that starts with a different number, the evaluation period restarts and you must assign a new license. For example, if you upgrade a vCenter Server system from 5.x to 6.x, you must license the system with a vCenter Server 6 license.

If you upgrade the edition of the license, for example, from vCenter Server Foundation to vCenter Server Standard, replace the existing license on the system with the upgraded license.

Licensing for Clusters with vSAN Enabled

After you enable vSAN on a cluster, you must assign the cluster an appropriate vSAN license.

Similar to vSphere licenses, vSAN licenses have per CPU capacity. When you assign a vSAN license to a cluster, the amount of license capacity used equals the total number of CPUs in the hosts participating in the cluster. For example, if you have a vSAN cluster that contains 4 hosts with 8 CPUs each, assign the cluster a vSAN license with a minimum capacity of 32 CPUs.

The license use of the vSAN is recalculated and updated in one of the following cases:

- If you assign a new license to the vSAN cluster
- If you add a new host to the vSAN cluster
- If a host is removed from the cluster
- If the total number of CPUs in a cluster changes

You must maintain the vSAN clusters in compliance with the vSAN licensing model. The total number of CPUs of all hosts in the cluster must not exceed the capacity of the vSAN license that is assigned to the cluster.

License and Evaluation Period Expiry

When the license or the evaluation period of a vSAN expires, you can continue to use the currently configured vSAN resources and features. However, you cannot add SSD or HDD capacity to an existing disk group or create new disk groups.

vSAN for Desktop

vSAN for Desktop is intended for use in VDI environments, such as vSphere for Desktop or Horizon ™View™. The license use for vSAN for Desktop equals the total number of powered on VMs in a cluster with enabled vSAN.

To remain EULA compliant, the license use for vSAN for Desktop must not exceed the license capacity. The number of powered on desktop VMs in a vSAN cluster must be less than or equal to the license capacity of vSAN for Desktop.

Licensing for vSphere with Tanzu

Once you configure a vSphere cluster for vSphere with Tanzu and it becomes a Supervisor Cluster, you must assign the cluster a Tanzu edition license before the 60 day evaluation period expires.

About the Tanzu Licenses

A Tanzu license enables the Workload Management functionality in vSphere 7.0 Update 1 and later. It is applicable to Supervisor Clusters that are configured with the vSphere networking stack or with NSX-T Data Center. For Supervisor Clusters running on vSphere 7.0, you need the VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes license assigned to each host from the Supervisor Cluster.

As a vSphere administrator, when you assign a Tanzu license to a Supervisor Cluster , you can create and configure namespaces and provide access to these namespaces to DevOps engineers. As a DevOps engineer, you can deploy Tanzu Kubernetes clusters and vSphere Pods inside the namespaces to which you have access. If the Supervisor Cluster is configured with the vSphere networking stack, you can only deploy Tanzu Kubernetes clusters in them.

Licensing a Supervisor Cluster

After you enable **Workload Management** on a vSphere cluster, which deploys a Supervisor Cluster, you can use the full set of capabilities of the cluster within a 60 day evaluation period. You must assign a Tanzu license to the Supervisor Cluster before the 60 day evaluation period expires.

If you configure NSX-T Data Center as the networking stack for the Supervisor Cluster, you must assign an NSX-T Data Center Advanced or higher license to NSX Manager. If you configure the Supervisor Cluster with the vSphere networking stack with NSX Advanced Load Balancer, you need an appropriate license for the load balancer depending on your Tanzu license edition.

If your environment runs on top of vSphere 7.0 and you upgrade the Supervisor Cluster to vSphere 7.0 Update 1 or later, the cluster enters evaluation mode after the upgrade completes. The VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes license that is assigned to the hosts acts as a regular vSphere Enterprise 7 Plus license, it does not enable any vSphere with Tanzu functionality. In that case, you must assign the Supervisor Cluster a Tanzu edition license before the 60 day evaluation period expires.

Tanzu License Expiration

- vSphere 7.0 Update 3. Starting from vSphere 7.0 Update 3, when a Tanzu edition license expires, you can continue using the full set of capabilities of vSphere with Tanzu until you procure new licenses. However, you cannot assign the expired license on new Supervisor Clusters. You must assign a valid Tanzu edition license to newly-created Supervisor Clusters before their 60 day evaluation period expires.
- vSphere 7.0 Update 2 and Update 1. When a Tanzu edition license expires in an environment that runs on vSphere Update 2 or Update 1, as a vSphere administrator you cannot create new namespaces or update the Kubernetes version of the Supervisor Cluster. As a DevOps engineer, you cannot deploy new workloads. You cannot change the configuration of the existing Tanzu Kubernetes clusters such as adding new nodes.

  You can still deploy workloads on Tanzu Kubernetes clusters and all existing workloads continue to run as expected. All Kubernetes workloads that are already deployed continue their normal operation.

Tanzu License Compliance

A Tanzu license key has per CPU capacity with up to 32 cores per CPU, similarly to the ESXi host licenses. When you assign a Tanzu license to a Supervisor Cluster, the amount of capacity consumed is determined by the number of CPUs on the hosts from the cluster and the number of cores in each CPU. You can assign a Tanzu edition license key to multiple Supervisor Clusters at a time, but you cannot assign multiple license keys to one cluster.

- vSphere 7.0 Update 3. Starting from vSphere 7.0 Update 3, if you expand a Supervisor Cluster by adding new hosts for example, and the license key that you have assigned to the cluster runs out of capacity, you can continue using the same license key. To remain EULA compliant however, you must procure a new license key with sufficient capacity to cover all the CPUs and cores in the Supervisor Cluster.
- vSphere 7.0 Update 2 and Update 1. If your vSphere with Tanzu environment runs on vSphere 7.0 Update 2 and Update 1, the total number of CPUs in a Supervisor Cluster must not exceed the amount of CPU capacity of the Tanzu edition license that is assigned to the cluster.

Evaluation Period Expiration

When the evaluation period for a Supervisor Cluster expires, as a vSphere administrator you cannot create new namespaces or update the Kubernetes version of the Supervisor Cluster. As a DevOps engineer, you cannot deploy new workloads and you cannot make changes to the configuration of the existing Tanzu Kubernetes clusters such as adding new nodes.

You can still deploy workloads on Tanzu Kubernetes clusters and all existing workloads continue to run as expected. All Kubernetes workloads that are already deployed continue their normal operation.

The evaluation period expiration behavior is valid for both vSphere 7.0 Update 2 and Update 3.

vSphere+ and vSAN+ Subscriptions

VMware vSphere+™ is a workload platform that allows you to shift from license based management to a pay-as-you-expand subscription model. If you plan on deploying vSAN clusters in a vSphere environment converted to subscription, you can either continue to use vSAN license keys or purchase a VMware vSAN+™ subscription in addition to the vSphere + subscription.

To learn more about how to convert your vCenter Server to subscription and start using the vSphere+ and vSAN+ features, see the *VMware vSphere+* documentation.

vSphere+ and vSAN+ Subscription

You can convert your vCenter Server instances to vSphere+ before the license evaluation period expires or before the assigned licenses to the vCenter Server and ESXi hosts expire.

If the vCenter Server instances that you plan to subscribe to vSphere+ manage vSAN clusters, you can either continue to use vSAN license keys or purchase a vSAN+ subscription. Do not use a combination of vSAN+ subscriptions and vSAN license keys within the same VMware Cloud account Organization. Combining vSAN+ subscriptions and vSAN license keys results in the entire vSAN deployment being converted to vSAN+ subscription metering and billing, where the license keys would be ignored. This could result in unexpected subscription usage.

When you deactivate vSAN on a cluster with a vSAN+ subscription, the vSphere+ subscription is applied automatically to all ESXi hosts associated with that cluster.

In the vSphere Client, you can view whether your vCenter Server instances are subscribed to vSphere+ and vSAN+. You can view your current subscription usage in the VMC Console. See Subscription Information for Your vCenter Server.

Free Trial

VMware offers a free trial subscription period for vSphere+ and vSAN+. When you are ready to purchase a vSphere+ subscription, contact a VMware sales representative or a VMware partner to help you plan converting your on-premises workloads to subscription. Subscriptions can be purchased for a period of one or three years.

When the free trial expires, you can no longer access the vSphere+ and vSAN+ features.

Subscription Information for Your vCenter Server

When your vCenter Server is converted to vSphere+ subscription, all license information is replaced with subscription information. For vSAN+ clusters, license information is replaced with subscription information.

If you have other VMware products with assigned licenses in your vCenter Server on subscription, you can view and manage their licenses in the vSphere Client. For example, if you want to turn a vSphere cluster to a Supervisor Cluster for running Kubernetes workloads, you can assign a Tanzu edition license by using the vSphere Client. See Licensing for vSphere with Tanzu.

View Subscription Information About Your vCenter Server

When you convert your vCenter Server instances to subscription, the vSphere Client shows your subscription information.

- Your vCenter Server instance must be converted to subscription.

1. In the vSphere Client home page, from the **Home** menu, click **Administration** > **Licensing & Subscription**.
2. Navigate to the licensing and subscription information.
   a) Click **Licenses** to view the license information about your vCenter Server.

      Since your vCenter Server is on subscription, you no longer need to add license keys for the vCenter Server instance and the ESXi hosts.

      You can assign licenses only to some assets, such as vSphere with Tanzu and VMware Site Recovery Manager. You license assets in the same way as for a vSphere environment using licensing.

      Note: When your vCenter Server is on subscription, the **Assets** tab no longer contains tabs that group the different VMware products. Instead, all assets to which you can assign a license are displayed in one pane.
   b) Click **Subscriptions** to view the subscription information for your vCenter Server instance.

      In the **Subscription** pane, click **View current usage** to open the VMC Console and view your current subscription usage. See *vSphere+ Documentation*.

      To view your billing information in the VMware Cloud Services Console™, click **View Billing**. See the *Billing & Subscription* chapter in the *Using VMware Cloud Services Console* documentation.

View Subscription Information About a vSAN Cluster

For a vSAN cluster on vSAN+ subscription, you can view subscription information in the vSphere Client.

- Your vCenter Server must be converted to subscription and vSAN+ subscription must be applied on all vSAN clusters in your vSphere+ environment.

1. In the vSphere Client, navigate to a vSAN cluster.
2. Click the **Configure** tab.
3. Under Licensing & Subscription, click **vSAN Cluster**.

   In the **vSAN Cluster Licensing** pane, you can view the subscription information for the selected vSAN cluster.

   For more information on subscription, see vSphere+ and vSAN+ Subscriptions

Managing Licenses

To license an asset in vSphere, you must assign it a license that holds an appropriate product license key. You can use the license management functionality in the vSphere Client to license multiple assets at a time from a central place. Assets are vCenter Server systems, hosts, vSAN clusters, Supervisor Clusters, and solutions.

In vSphere, you can assign one license to multiple assets of the same type if the license has enough capacity. You can assign a suite license to all components that belong to the suite product edition. For example, you can assign one vSphere license to multiple ESXi hosts, but you cannot assign two licenses to one host. If you have a vCloud Suite license, you can assign the license to ESXi hosts, vCloud Networking and Security, vCenter Site Recovery Manager, and so on.

Create New Licenses

When you purchase, divide, or combine license keys in Customer Connect, you must use the new keys to license assets in your vSphere environment. You must go to the vSphere Client and create a license object for every license key. A license is a container for a license key of a VMware product. After you create the new licenses, you can assign them to assets.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. On the **Licenses** tab, click **Add New Licenses**.
4. On the Enter licenses keys page, enter one license key per line, and click **Next**.
   The license key is a 25-symbol string of letters and digits in the format `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`. You can enter a list of keys in one operation. A new license will be created for every license key that you enter.
5. On the Edit license names page, rename the new licenses as appropriate and click **Next** .
6. On the Ready to complete page, review the new licenses and click **Finish**.

A new license is created for every license key that you entered.

Assign the new licenses to hosts, vCenter Server systems, or other products that you use with vSphere. You must not keep unassigned licenses in the inventory.

Configuring License Settings for Assets in the vSphere Client

To continue using product functionality, you must assign appropriate licenses to assets in evaluation mode, or assets with expiring licenses. When you upgrade a license edition, combine, or split licenses in Customer Connect, you must assign the new licenses to assets. You can assign licenses that are already available or create licenses and assign them to the assets in a single workflow. Assets are vCenter Server systems, ESXi hosts, vSAN clusters, Supervisor Clusters, and other products that integrate with vSphere.

Assign a License to Multiple Assets

To continue using product functionality, you must assign appropriate licenses to assets in evaluation mode, or assets with expiring licenses. When you upgrade a license edition, combine, or split licenses in Customer Connect, you must assign the new licenses to assets. You can assign licenses that are already available, or create licenses and assign them to the assets in a single workflow. Assets are vCenter Server systems, ESXi hosts, vSAN clusters, Supervisor Clusters, and other products that integrate with vSphere.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select the **Assets** tab.
4. On the **Assets** tab, click the **vCenter Server systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, or **Solutions** tab.
5. Select the assets to license.

   Note: Use Shift+click to select multiple assets.
6. Click **Assign License**.
7. In the **Assign License** dialog box, select the task that you want to perform.
   - In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
----------	----------
Select a newly created license	1. Click the **New License** tab. 2. In the **Assign License** dialog box, type or copy and paste a license key and click **OK**. 3. Enter a name for the new license and click **OK**. Details about the product, product features, capacity, and expiration period appear on the page. 4. Click **OK**. 5. In the **Assign License** dialog box, select the newly created license, and click **OK**.

The license is assigned to the assets. Capacity from the license is allocated according to the license use of the assets. For example, if you assign the license to 3 hosts with 4 CPUs each, the consumed license capacity is 12 CPUs.

Configure License Settings for an ESXi Host

You must assign a license to an ESXi host before its evaluation period expires or its currently assigned license expires. If you upgrade, combine, or divide vSphere licenses in Customer Connect, you must assign the new licenses to ESXi hosts and remove the old licenses.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Navigate to the host in the inventory.
2. Select the **Configure** tab.
3. Under **Settings**, select **Licensing**.
4. Click **Assign License**.
5. In the **Assign License** dialog box, select the task that you want to perform.
   - In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
----------	**----------**
Select a newly created license	1. Click the **New License** tab. 2. In the **Assign License** dialog box, type or copy and paste a license key and click **OK**. 3. Enter a name for the new license and click **OK**. Details about the product, product features, capacity, and expiration period appear on the page. 4. Click **OK**. 5. In the **Assign License** dialog box, select the newly created license, and click **OK**.

The license is assigned to the host. Capacity from the license is allocated according to the license use of the host.

Configure License Settings for vCenter Server

You must assign a license to a vCenter Server system before its evaluation period expires or its currently assigned license expires. If you upgrade, combine, or divide vCenter Server licenses in Customer Connect, you must assign the new licenses to vCenter Server systems and remove the old licenses.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **Licensing**.
4. Click **Assign License**.
5. In the **Assign License** dialog box, select the task that you want to perform.
   - In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click **OK**.
----------	**----------**
Select a newly created license	1. Click the **New License** tab. 2. In the **Assign License** dialog box, type or copy and paste a license key and click **OK**.

Task	Steps
	3. Enter a name for the new license and click **OK**. Details about the product, product features, capacity, and expiration period appear on the page. 4. Click **OK**. 5. In the **Assign License** dialog box, select the newly created license, and click **OK**.

The license is assigned to the vCenter Server system, and one instance from the license capacity is allocated for the vCenter Server system.

Configure License Settings for a vSAN Cluster

You must assign a license to a vSAN cluster before its evaluation period expires or its currently assigned license expires.

- To view and manage vSAN licenses, you must have the **Global** > **Licenses** privilege on the vCenter Server systems.

If you upgrade, combine, or divide vSAN licenses, you must assign the new licenses to vSAN clusters. When you assign a vSAN license to a cluster, the amount of license capacity used equals the total number of CPUs in the hosts participating in the cluster. The license use of the vSAN cluster is recalculated and updated every time you add or remove a host from the cluster. For information about managing licenses and licensing terminology and definitions, see the *vCenter Server and Host Management* documentation.

When you enable vSAN on a cluster, you can use vSAN in evaluation mode to explore its features. The evaluation period starts when vSAN is enabled, and expires after 60 days. To use vSAN, you must license the cluster before the evaluation period expires. Just like vSphere licenses, vSAN licenses have per CPU capacity. Some advanced features, such as all-flash configuration and stretched clusters, require a license that supports the feature.

1. Navigate to your vSAN cluster.
2. Click the **Configure** tab.
3. Under Licensing, select **vSAN Cluster**.
4. Click Assign License.
5. Select an existing license and click **OK**.

Assign the Tanzu Edition License to a Supervisor Cluster

If you are using a Supervisor Cluster in evaluation mode, you must assign the cluster a Tanzu edition license before the 60 day evaluation period expires.

Note: If the evaluation period of a Supervisor Cluster expires, or the Tanzu edition license expires, as a vSphere administrator you cannot create any new namespaces on the Supervisor Cluster, or update the Kubernetes version of the cluster. As a DevOps engineer, you cannot create new vSphere Pods, VMs, and Tanzu Kubernetes clusters. You cannot update the configuration of the existing Tanzu Kubernetes clusters, such as adding new nodes. All Kubernetes

workloads that are already deployed continue their normal operation and you can deploy new workloads on the existing Tanzu Kubernetes clusters.

1. In the vSphere Client, navigate to the Supervisor Cluster.
2. Select **Configure** and under **Licensing** select **Supervisor Cluster**.
3. Select **Assign License**.
4. In the **Assign License** dialog, click **New License**.
5. Enter a valid license key and click **OK**.

Set Assets to Evaluation Mode

To explore the complete set of features available for an asset, you can set it to evaluation mode.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

Different products have different terms for using their evaluation mode. Before you set an asset to evaluation mode, you should consider the specifics for using the evaluation mode of its associated product. For details, see the licensing model documentation for the relevant product at Licensing and Subscription for Products in vSphere.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select the **Assets** tab.
4. Select the **vCenter Server systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, or **Solutions** tab.
5. Select the asset that you want to set to evaluation mode.
6. Click the **Assign License** icon.
7. Select **Evaluation License** and click **OK** to save your changes.

The asset is in evaluation mode. You can explore the entire set of features that are available for the asset.

Note: You must assign an appropriate license to the asset before its evaluation period expires. Otherwise the asset gets into unlicensed state and certain functionality will be blocked.

Rename a License

After you create a license, you can change its name.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select the **Licenses** tab.
4. Select the license to rename, and click **Rename License**.
5. Type the new license name and click **OK**.

Remove Licenses

To remain in compliance with the licensing models of products that you use with vSphere, you must remove all unassigned licenses from the inventory. If you have divided, combined, or upgraded licenses in Customer Connect, you must remove the old licenses.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

For example, suppose that you have upgraded a vSphere license from 6.7 to 7.0 in Customer Connect. You assign the license to ESXi 7.0 hosts. After assigning the new vSphere 7.0 licenses, you must remove the old vSphere 6.7 license from the inventory.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select the **Licenses** tab.
4. Use the filters to display only the unassigned licenses.
5. Click the filter icon ( ) in the **State** column.
   A text box appears.
6. Select what licenses you want to display (unassigned or assigned).
7. Select a license to remove or press Ctrl+A to select all licenses.
8. Click **Remove Licenses**, review the confirmation message, and click **Yes**.

Viewing Licensing Information

You can view the licensing state of the vSphere environment from a central place by using the license management functionality in the vSphere Client . You can view the licenses that are available in vSphere, current license assignments and usage, available license capacity, licensed features in use, and so on.

You can also export information about licenses and their expiration dates, capacity, and usage. You can export data about the available products and assets in the vSphere Client by downloading a `.CSV` file.

View Licensing Information About the vSphere Environment

You can view the available licenses in vSphere and their expiration dates, available capacity, and usage. You can also view the available products and assets.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select a tab for the licensing information that you want to view.

Tab	Description
Licenses	Lists all licenses that are available in the vSphere environment. For every license, you can view the associated license key, license usage, license capacity, and expiration date.
Products	Lists the products that have licenses available in the vSphere environment. You can view the licenses that are

Tab	Description
	available for every product, licensed features, license usage, and license capacity.
Assets	Displays licensing information about the assets that are available in the vSphere environment. Assets are vCenter Server systems, hosts, vSAN clusters, Supervisor Clusters, and other products that you use with vSphere that are listed under Solutions.

If you have upgraded, divided, or combined any licenses in Customer Connect, you must not use these old license keys and should remove them from the inventory.

View Available Licenses and Features About a Product

You can view information about a product, such as the available licenses, features, and license capacity in the vSphere Client.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Click the **Products** tab and select the product for which you want to view information.
4. Select the task that you want to perform.

Task	Description
View the licenses that are available for the selected product	In the vSphere Client, click the **Licenses** subtab below the list of products.
View the licensed features for the product	In the vSphere Client, click the **Features** subtab below the list of products.

View the Features That an Asset Can Use

You can view the features that an asset can use based on the license that is assigned to it.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select the **Assets** tab.
4. Select the **vCenter Server systems**, **Hosts**, **vSAN Clusters**, **Supervisor Clusters**, or the **Solutions** option.
5. Select an asset and view the associated features.
6. Click the **Features** subtab below the list of assets.

View the License Key of the License

In vSphere, a license holds a license key for a product. You can view the associated license key for every license.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Select the **Licenses** tab.
4. Select a license from the list and view the license key.
5. Click the **Summary** subtab that is below the list of licenses. Under General, you can see the license name, the expiration date, the state of the license, and the license key.

View the Licensed Features for an Asset

Before you start to use a feature on an asset, you can check whether the asset is licensed to use this feature. For example, to use vSphere HA, you must check whether all hosts in a vSphere HA cluster are licensed for this feature.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Navigate to the vCenter Server system, host, or cluster whose licensed features you want to view.
2. Click the **Configure** tab.
3. Under Settings, select **Licensing**.

The list of features that you can configure on the asset appears on the right.

Export Licensing Information in the vSphere Environment

You can export licensing information about vSphere licenses, products, or assets. The information is saved on your local system as a `.CSV` file. You can later open the `.CSV` file with third-party applications.

- To view and manage licenses in the vSphere environment, you must have the **Global** > **Licenses** privilege on the system, where the vSphere Client runs.

1. Click **Menu** > **Administration**.
2. Expand **Licensing** and click **Licenses**.
3. Optional: Select an item to export.
   - Click the **Licenses** tab to select one or more licenses to export.
   - Click the **Products** tab to select a product to export.
   - Click the **Assets** tab to select the vCenter Server instance, hosts, clusters, or solutions whose licensing information you want to export.

   If you do not select a particular license, product, or asset, all items from the respective list are exported.
4. Export the items.

   When prompted, save the CSV file on your file system.
   - If you selected one or more items to export, click **Export** and select **Selected Rows**.
   - If you selected one or more items but you want to export all items, click **Export** and select **All Rows**.
   - If you selected no items, click **Export**.

vCenter Server Domain Repoint License Considerations

Domain repointing copies license keys to a new domain. Copying the license keys ensures that valid licensing of all assets is maintained after repointing.

vCenter Server tracks license usage on a per domain basis. If a key is used in more than one domain, you must ensure that the aggregate use of the key does not exceed its capacity. To simplify your license management, remove each license copied to a second domain and assign a new license to assets.

Consider the following two cases:

- License keys that are no longer in use (that is, assigned to assets) in the original domain post repointing.
- License keys that are in use (that is, assigned to assets) in multiple domains.

License Keys Not in Use in a Domain

License Keys in Use in Multiple Domains

If after completing repointing, a license key is in use (that is, assigned to assets) in more than one domain, to remove the license key from all but one domain, first a different license key must be assigned to each asset in domains from which the license key will be removed. Two common approaches:

Migrating Virtual Machines

You can move virtual machines from one compute resource or storage location to another by using cold or hot migration. For example, with vSphere vMotion you can move powered on virtual machines away from a host to perform maintenance, to balance loads, to collocate virtual machines that communicate with each other, to move virtual machines apart to minimize fault domain, to migrate to new server hardware, and so on.

Moving a virtual machine from one inventory folder to another folder or resource pool in the same data center is not a form of migration. Unlike migration, cloning a virtual machine or copying its virtual disks and configuration file in the same vCenter Server system are procedures that create a new virtual machine. Cloning and copying a virtual machine in the same vCenter Server system are also not forms of migration.

By using migration, you can change the compute resource that the virtual machine runs on. For example, you can move a virtual machine from one host to another host or cluster.

To migrate virtual machines with disks larger than 2 TB, the source and destination ESXi hosts must be version 6.0 and later.

Depending on the power state of the virtual machine that you migrate, migration can be cold or hot.

Cold Migration	Moving a powered off or suspended virtual machine to a new host. Optionally, you can relocate configuration and disk files for powered off or suspended virtual machines to new storage locations. You can also use cold migration to move virtual machines from one virtual switch to another, and from one data center to another. You can perform cold migration manually or you can schedule a task.
Hot Migration	Moving a powered on virtual machine to a new host. Optionally, you can also move the virtual machine disks or folder to a different datastore. Hot migration is also called live migration or vSphere vMotion. With vSphere vMotion, you migrate the virtual machine without any interruption in its availability.

Depending on the virtual machine resource type, you can perform three types of migration.

Change compute resource only	Moving a virtual machine, but not its storage, to another compute resource, such as a host, cluster, resource pool, or vApp. You can move the virtual machine to another compute resource by using cold or hot migration. If you change the compute resource of a powered on virtual machine, you use vSphere vMotion.
Change storage only	Moving a virtual machine and its storage, including virtual disks, configuration files, or a combination of these, to a new datastore on the same host. You can change the datastore of a virtual machine by using cold or hot migration. If you move a powered on virtual machine and its storage to a new datastore, you use Storage vMotion.
Change both compute resource and storage	Moving a virtual machine to another host and at the same time moving its disk or virtual machine folder to another datastore. You can change the host and datastore simultaneously by using cold or hot migration.

In vSphere 6.0 and later, you can move virtual machines between vSphere sites by using migration between the following types of objects.

Migrate to another virtual switch	Moving the network of a virtual machine to a virtual switch of a different type. You can migrate virtual machines without reconfiguring the physical and virtual network. By using cold or hot migration, you can move the virtual machine from a standard to a standard or distributed switch, and from a distributed switch

	to another distributed switch. When you move a virtual machine network between distributed switches, the network configuration and policies that are associated with the network adapters of the virtual machine are transferred to the target switch.
Migrate to another data center	Moving a virtual machine to a different data center. You can change the data center of a virtual machine by using cold or hot migration. For networking in the target data center, you can select a dedicated port group on a distributed switch.
Migrate to another vCenter Server system	Moving a virtual machine to a different vCenter Server instance. You can move a virtual machine to a vCenter Server instance that is connected to the source vCenter Server instance through vCenter Enhanced Linked Mode. You can also move virtual machines between vCenter Server instances that are located across a long distance from each other. Starting with vSphere 7.0 Update 1c, you can migrate workloads across vCenter Server systems by using Advanced Cross vCenter vMotion. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains. Starting with vSphere 7.0 Update 3, you can use the Advanced Cross vCenter vMotion feature to clone virtual machines across vCenter Server systems.

Cold Migration

Cold migration is the migration of powered off or suspended virtual machines between hosts across clusters, data centers, and vCenter Server instances. By using cold migration, you can also move associated disks from one datastore to another.

You can use cold migration to have the target host checked against fewer requirements than when you use vMotion. For example, if you use cold migration when a virtual machine contains a complex application setup, the compatibility checks during vMotion might prevent the virtual machine from moving to another host.

You must power off or suspend the virtual machines before you begin the cold migration process. Migrating a suspended virtual machine is considered a cold migration because although the virtual machine is powered on, it is not running.

Migrating a virtual machine across its network subnets may result in the loss of network connectivity.

CPU Compatibility Check During Cold Migration

If you attempt to migrate a powered off virtual machine that is configured with a 64-bit operating system to a host that does not support 64-bit operating systems, vCenter Server generates a warning. Otherwise, CPU compatibility checks do not apply when you migrate powered off virtual machines with cold migration.

When you migrate a suspended virtual machine, the new host for the virtual machine must meet CPU compatibility requirements. This requirement allows the virtual machine to resume execution on the new host.

Operations During Cold Migration

A cold migration consists of the following operations:

1. If you select the option to move to a different datastore, the configuration files, including the NVRAM file (BIOS settings), log files, and the suspend file, are moved from the source host to the destination host’s associated storage area. You can choose to move the virtual machine's disks as well.

2. The virtual machine is registered with the new host.
3. After the migration is completed, the old version of the virtual machine is deleted from the source host and datastore if you selected the option to move to a different datastore.

Network Traffic for Cold Migration

By default, data for VM cold migration, cloning, and snapshots is transferred through the management network. This traffic is called provisioning traffic. It is not encrypted but uses run-length encoding of data.

On a host, you can dedicate a separate VMkernel network adapter to the provisioning traffic, for example, to isolate this traffic on another VLAN. On a host, you can assign no more than one VMkernel adapter for provisioning traffic. For information about enabling provisioning traffic on a separate VMkernel adapter, see the *vSphere Networking* documentation.

If you plan to transfer high volumes of virtual machine data that the management network cannot accommodate, redirect the cold migration traffic on a host to the TCP/IP stack that is dedicated to cold migration and cloning of powered off virtual machines. You can also redirect if you want to isolate cold migration traffic in a subnet different from the management network, for example, for migration over a long distance. See How to Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.

Migration with vMotion

If you must take a host offline for maintenance, you can move the virtual machine to another host. Migration with vSphere vMotion allows virtual machine processes to continue working throughout a migration.

When you migrate a virtual machine with vMotion, the new host for the virtual machine must meet compatibility requirements so that the migration can proceed.

vMotion Migration Types

With vMotion, you can change the compute resource on which a virtual machine is running. You also can change both the compute resource and the storage of the virtual machine.

When you migrate virtual machines with vMotion and choose to change only the host, the entire state of the virtual machine is moved to the new host. The associated virtual disk remains in the same location on storage that must be shared between the two hosts.

When you choose to change both the host and the datastore, the virtual machine state is moved to a new host and the virtual disk is moved to another datastore. vMotion migration to another host and datastore is possible in vSphere environments without shared storage.

After the virtual machine state is migrated to the alternate host, the virtual machine runs on the new host. Migrations with vMotion are transparent to the running virtual machine.

When you choose to change both the compute resource and the storage, you can use vMotion to migrate virtual machines across vCenter Server instances, data centers, and subnets.

Transferred State Information

The state information includes the current memory content and all the information that defines and identifies the virtual machine. The memory content includes transaction data and the bits of the operating system and applications that are in the memory. The defining and identification information stored in the state includes all the data that maps to the virtual machine hardware elements. This information includes BIOS, devices, CPU, MAC addresses for the Ethernet cards, chipset states, registers, and so forth.

Stages in vMotion

Migration with vMotion occurs in three stages:

1. When the migration with vMotion is requested, vCenter Server verifies that the existing virtual machine is in a stable state with its current host.
2. The virtual machine state information (memory, registers, and network connections) is copied to the target host.
3. The virtual machine resumes its activities on the new host.

If errors occur during migration, the virtual machine reverts to its original state and location.

Host Configuration for vMotion

Before using vMotion, you must configure your hosts correctly.

- Each host must be licensed for vMotion.
- Each host must meet shared storage requirements for vMotion. See vMotion Shared Storage Requirements.
- Each host must meet the networking requirements for vMotion. See vSphere vMotion Networking Requirements.

vMotion Across Long Distances

You can perform reliable migrations between hosts and sites that are separated by high network round-trip latency times. vMotion across long distances is enabled when the appropriate license is installed. No user configuration is necessary.

For long-distance migration, verify the network latency between the hosts and your license.

- The round-trip time between the hosts must be up to 150 milliseconds.
- Your license must cover vMotion across long distances.
- You must place the traffic related to transfer of virtual machine files to the destination host on the provisioning TCP/IP stack. See How to Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.

vMotion Shared Storage Requirements

Configure hosts for vMotion with shared storage to ensure that virtual machines are accessible to both source and target hosts.

During a migration with vMotion, the migrating virtual machine must be on storage accessible to both the source and target hosts. Ensure that the hosts configured for vMotion use shared storage. Shared storage can be on a Fibre Channel storage area network (SAN), or can be implemented using iSCSI and NAS.

If you use vMotion to migrate virtual machines with raw device mapping (RDM) files, make sure to maintain consistent LUN IDs for RDMs across all participating hosts.

See the *vSphere Storage* documentation for information on SANs and RDMs.

vSphere vMotion Networking Requirements

Migration with vMotion requires correctly configured network interfaces on source and target hosts.

Configure each host with at least one network interface for vMotion traffic. To ensure secure data transfer, the vMotion network must be a secure network, accessible only to trusted parties. Additional bandwidth significantly improves vMotion performance. When you migrate a virtual machine with vMotion without using shared storage, the contents of the virtual disk is transferred over the network as well.

vSphere 6.5 and later allow the network traffic with vMotion to be encrypted. Encrypted vMotion depends on host configuration, or on compatibility between the source and destination hosts.

Requirements for Concurrent vMotion Migrations

You must ensure that the vMotion network has at least 250 Mbps of dedicated bandwidth per concurrent vMotion session. Greater bandwidth lets migrations complete more quickly. Gains in throughput resulting from WAN optimization techniques do not count towards the 250-Mbps limit.

To determine the maximum number of concurrent vMotion operations possible, see Limits on Simultaneous Migrations. These limits vary with a host's link speed to the vMotion network.

Round-Trip Time for Long-Distance vMotion Migration

If you have the proper license applied to your environment, you can perform reliable migrations between hosts that are separated by high network round-trip latency times. The maximum supported network round-trip time for vMotion migrations is 150 milliseconds. This round-trip time lets you migrate virtual machines to another geographical location at a longer distance.

Multiple-NIC vMotion

You can configure multiple NICs for vMotion by adding two or more NICs to the required standard or distributed switch. For details, see Knowledge Base article KB 2007467.

Network Configuration

Configure the virtual networks on vMotion enabled hosts as follows:

- On each host, configure a VMkernel port group for vMotion.
  To have the vMotion traffic routed across IP subnets, enable the vMotion TCP/IP stack on the host. See Place vMotion Traffic on the vMotion TCP/IP Stack of an Host.
- If you are using standard switches for networking, ensure that the network labels used for the virtual machine port groups are consistent across hosts. During a migration with vMotion, vCenter Server assigns virtual machines to port groups based on matching network labels.
  Note:

  By default, you cannot use vMotion to migrate a virtual machine that is attached to a standard switch with no physical uplinks configured, even if the destination host also has a no-uplink standard switch with the same label.

  To override the default behavior, set the `config.migrate.test.CompatibleNetworks.VMOnVirtualIntranet` advanced settings of vCenter Server to `false`. The change takes effect immediately. For information about configuring advanced settings of vCenter Server, see *vCenter Server Configuration*.
- If you use Intrusion Detection Systems (IDS) and firewalls to protect your environment, make sure that you configure them to allow connections to the ports used for vMotion on the ESXi hosts. For the list of currently supported ports for vMotion, see the VMware Ports and Protocols Tool™ at https://ports.esp.vmware.com/home/vSphere.

For information about configuring the vMotion network resources, see Networking Best Practices for vSphere vMotion .

For more information about vMotion networking requirements, see Knowledge Base article KB 59232.

Networking Best Practices for vSphere vMotion

Consider certain best practices for configuring the network resources for vMotion on an ESXi host.

- Provide the required bandwidth in one of the following ways:

Physical Adapter Configuration	Best Practices
Dedicate at least one adapter for vMotion or reserve network bandwidth for vMotion.	Use at least one 10 GbE adapter for workloads that have a small number of memory operations, or if you migrate workloads that have many memory operations. If only two Ethernet adapters are available, for best availability, combine both adapters into a team, and use VLANs to divide traffic into networks: one or more for virtual machine traffic and one for vMotion. Alternatively, you can reserve at least 10 Gbps of network bandwidth for vMotion on a high speed link.
Direct vMotion traffic to one or more physical NICs that have high-bandwidth capacity and are shared between other types of traffic as well	• To distribute and allocate more bandwidth to vMotion traffic across several physical NICs, use multiple-NIC vMotion. • On a vSphere Distributed Switch 5.1 and later, use vSphere Network I/O Control shares to guarantee bandwidth to outgoing vMotion traffic. Defining shares also prevents from contention as a result from excessive vMotion or other traffic. • In vSphere 7.0 Update 1 or earlier, vMotion saturates 1 GbE and 10 GbE physical NICs with a single vMotion VMkernel NIC. Starting with vSphere 7.0 Update 2, vMotion saturates high speed links such as 25 GbE, 40 GbE and 100 GbE with a single vMotion VMkernel NIC. If you do not have dedicated uplinks for vMotion, you can use Network I/O Control to limit vMotion bandwidth use. • To avoid saturation of the physical NIC link as a result of intense incoming vMotion traffic, use traffic shaping in egress direction on the vMotion port group on the destination host. By using traffic shaping you can limit the average and peak bandwidth available to vMotion traffic, and reserve resources for other traffic types.

- Use jumbo frames for best vMotion performance.
  Ensure that jumbo frames are enabled on all network devices that are on the vMotion path including physical NICs, physical switches, and virtual switches.
- Place vMotion traffic on the vMotion TCP/IP stack for migration across IP subnets that have a dedicated default gateway that is different from the gateway on the management network. See Place vMotion Traffic on the vMotion TCP/IP Stack of an Host.

For information about configuring networking on an ESXi host, see the *vSphere Networking* documentation.

Encrypted vSphere vMotion

vSphere vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options.

Encrypted vSphere vMotion secures confidentiality, integrity, and authenticity of data that is transferred with vSphere vMotion. vSphere supports encrypted vMotion of unencrypted and encrypted virtual machines across vCenter Server instances.

What Is Encrypted

For encrypted disks, the data is transmitted encrypted in all cases. For unencrypted disks, the following applies:

- If disk data is transferred within a host, that is without changing the host, you change only the datastore, the transfer is unencrypted.

- If disk data is transferred between hosts and encrypted vMotion is used, the transfer is encrypted. If encrypted vMotion is not used the transfer is unencrypted.

For virtual machines that are encrypted, migration with vSphere vMotion always uses encrypted vSphere vMotion. You cannot turn off encrypted vSphere vMotion for encrypted virtual machines.

Encrypted vSphere vMotion States

For virtual machines that are not encrypted, you can set encrypted vSphere vMotion to one of the following states. The default is Opportunistic.

Disabled	Do not use encrypted vSphere vMotion.
Opportunistic	Use encrypted vSphere vMotion if source and destination hosts support it. Only ESXi versions 6.5 and later use encrypted vSphere vMotion.
Required	Allow only encrypted vSphere vMotion. If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.

When you encrypt a virtual machine, the virtual machine keeps a record of the current encrypted vSphere vMotion setting. If you later activated encryption for the virtual machine, the encrypted vMotion setting remains at Required until you change the setting explicitly. You can change the settings using **Edit Settings**.

Note:

Currently, you must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances. See *vSphere Web Services SDK Programming Guide* and *vSphere Web Services API Reference*.

Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances

vSphere vMotion supports migrating and cloning encrypted virtual machines across vCenter Server instances.

When migrating or cloning encrypted virtual machines across vCenter Server instances, the source and destination vCenter Server instances must be configured to share the key provider that was used to encrypt the virtual machine. In addition, the key provider name must be the same on both the source and destination vCenter Server instances and have the following characteristics:

- Standard key provider: The same key server (or key servers) must be in the key provider.
- Trusted key provider: The same vSphere Trust Authority service must be configured on the destination host.
- vSphere Native Key Provider: Must have the same KDK.

The destination vCenter Server ensures the destination ESXi host has encryption mode enabled, ensuring the host is cryptographically "safe."

The following privileges are required when using vSphere vMotion to migrate or clone an encrypted virtual machine across vCenter Server instances.

- Migrating: **Cryptographic operations** > **Migrate** on the virtual machine
- Cloning: **Cryptographic operations** > **Clone** on the virtual machine

Also, the destination vCenter Server must have the **Cryptographic operations** > **EncryptNew** privilege. If the destination ESXi host is not in "safe" mode, the **Cryptographic operations** > **RegisterHost** privilege must also be on the destination vCenter Server.

Certain tasks are not allowed when migrating virtual machines (non-encrypted or encrypted), either on the same vCenter Server or across vCenter Server instances.

- You cannot change the VM Storage Policy.
- You cannot perform a key change.

Note:

You can change the VM Storage Policy while cloning virtual machines.

Minimum Requirements for Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances

The minimum version requirements for migrating or cloning standard key provider encrypted virtual machines across vCenter Server instances using vSphere vMotion are:

- Both the source and destination vCenter Server instances must be on version 7.0 or later.
- Both the source and destination ESXi hosts must be on version 6.7 or later.

The minimum version requirements for migrating or cloning trusted key provider encrypted virtual machines across vCenter Server instances using vSphere vMotion are:

- The vSphere Trust Authority service must be configured for the destination host and the destination host must be attested.
- Encryption cannot change on migration. For example, an unencrypted disk cannot be encrypted while the virtual machine is migrated to the new storage.
- You can migrate a standard encrypted virtual machine onto a Trusted Host. The key provider name must be the same on both the source and destination vCenter Server instances.
- You cannot migrate a vSphere Trust Authority encrypted virtual machine onto a non-Trusted Host.

Trusted Key Provider vMotion and Cross-vCenter Server vMotion

Trusted key provider fully supports vMotion across ESXi hosts.

Cross-vCenter Server vMotion is supported, but with the following restrictions.

1. The required trusted service must be configured on the destination host and the destination host must be attested.
2. Encryption cannot change on migration. For example, a disk cannot be encrypted while the virtual machine is migrated to the new storage.

When performing cross-vCenter Server vMotion, vCenter Server checks that the trusted key provider is available on the destination host, and if the host has access to it.

vSphere Native Key Provider vMotion and Cross-vCenter Server vMotion

vSphere Native Key Provider supports vMotion and Encrypted vMotion across ESXi hosts. Cross-vCenter Server vMotion is supported if vSphere Native Key Provider is configured on the destination host.

Enable Encrypted vMotion on a Virtual Machine

You can enable encrypted vMotion during virtual machine creation. You can later change the encrypted vMotion state from the virtual machine settings. You can change the encrypted vMotion state only for virtual machines that are not encrypted.

Encrypted vMotion is supported only in vSphere 6.5 and later.

For more information about virtual machine encryption, see Encrypted vSphere vMotion.

1. Right-click the virtual machine and select **Edit Settings**.
2. Select **VM Options**.
3. Click **Encryption**, and select an option from the **Encrypted VMotion** drop-down menu.

Disabled	Do not use encrypted vMotion.

Opportunistic	Use encrypted vMotion if source and destination hosts support it. Only ESXi hosts of version 6.5 and later use encrypted vMotion.
Required	Allow only encrypted vMotion. If the source or destination host does not support encrypted vMotion, migration with vMotion fails.

Virtual Machine Conditions and Limitations for vMotion

To migrate virtual machines with vMotion, the virtual machine must meet certain network, disk, CPU, USB, and other device requirements.

The following virtual machine conditions and limitations apply when you use vMotion:

- The source and destination management network IP address families must match. You cannot migrate a virtual machine from a host that is registered to vCenter Server with an IPv4 address to a host that is registered with an IPv6 address.
- Using 1 GbE network adapters for the vMotion network might result in migration failure, if you migrate virtual machines with large vGPU profiles. Use 10 GbE network adapters for the vMotion network.
- If virtual CPU performance counters are enabled, you can migrate virtual machines only to hosts that have compatible CPU performance counters.
- You can migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use the graphics renderer that is present on the destination host. The renderer can be the host CPU or a GPU graphics card. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU graphics card.
- Starting with vSphere 6.7 Update 1 and later, vSphere vMotion supports virtual machines with vGPU.
- vSphere DRS supports initial placement of vGPU virtual machines running vSphere 6.7 Update 1 or later without load balancing support.
- You can migrate virtual machines with USB devices that are connected to a physical USB device on the host. You must enable the devices for vMotion.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device that is not accessible on the destination host. For example, you cannot migrate a virtual machine with a CD drive backed by the physical CD drive on the source host. Disconnect these devices before you migrate the virtual machine.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device on the client computer. Disconnect these devices before you migrate the virtual machine.
- You can simultaneously migrate virtual machines at a certain network, host, and datastore resource cost. When a resource exceeds its maximum cost, new migration operations are queued until the required resources are available. See Limits on Simultaneous Migrations.

Using vMotion to Migrate vGPU Virtual Machines

You can use vMotion to perform a live migration of NVIDIA vGPU-powered virtual machines without causing data loss.

To enable vMotion for vGPU virtual machines, you need to set the `vgpu.hotmigrate.enabled` advanced setting to `true` . For more information about how to configure the vCenter Server advanced settings, see *Configure Advanced Settings* in the *vCenter Server Configuration* documentation.

In vSphere 6.7 Update 1 and vSphere 6.7 Update 2, when you migrate vGPU virtual machines with vMotion and vMotion stun time exceeds 100 seconds, the migration process might fail for vGPU profiles with 24 GB frame buffer size or larger. To avoid the vMotion timeout, upgrade to vSphere 6.7 Update 3 or later.

During the stun time, you are unable to access the VM, desktop, or application. Once the migration is completed, access to the VM resumes and all applications continue from their previous state. For information on frame buffer size in vGPU profiles, refer to the NVIDIA Virtual GPU documentation.

The expected VM stun times (the time when the VM is inaccessible to users during vMotion) and the estimated worst-case stun times are listed in the following tables. The expected stun times were tested over a 10Gb network with NVIDIA Tesla V100 PCIe 32 GB GPUs:

Table 145: Expected Stun Times for vMotion of vGPU VMs

Used vGPU Frame Buffer (GB)	VM Stun Time (sec)
1	2
2	4
4	6
8	12
16	22
32	39

Table 146: Estimated Worst-Case Stun Times (sec)

vGPU Memory	VM Memory 4 GB	VM Memory 8 GB	VM Memory 16 GB	VM Memory 32 GB
1 GB	5	6	8	12
2 GB	7	9	11	15
4 GB	13	14	16	21
8 GB	24	25	28	32
16 GB	47	48	50	54
32 GB	91	92	95	99

Note: When you consider the expected and estimated worst-case stun times, keep in mind the following points:

- The configured vGPU profile represents an upper bound to the used vGPU frame buffer. In many use cases, the amount of vGPU frame buffer memory used by the VM at any given time is below the assigned vGPU memory in the profile.
- Both expected and estimated worst-case stun times are only valid when migrating a single virtual machine. If you are concurrently migrating multiple virtual machines, that is, for a vSphere manual remediation process, the stun times will have adverse effects.
- The above estimates assume sufficient CPU, memory, PCIe, and network capacity to achieve 10 Gbps migration throughput.

DRS supports initial placement of vGPU VMs running vSphere 6.7 Update 1 and later without load balancing support.

VMware vSphere vMotion is supported only with and between compatible NVIDIA GPU device models and NVIDIA GRID host driver versions as defined and supported by NVIDIA. For compatibility information, refer to the NVIDIA Virtual GPU User Guide.

To check compatibility between NVIDIA vGPU host drivers, vSphere, and Horizon, refer to the Broadcom Compatibility Guide.

Related tasks

- Migrate a Virtual Machine to a New Compute Resource
- Migrate a Virtual Machine to a New Compute Resource and Storage
- Migrate a Virtual Machine to New Storage

Swap File Location Compatibility

Virtual machine swap file location affects vMotion compatibility in different ways depending on the version of ESXi running on the virtual machine's host.

You can configure ESXi 6.5 or later hosts to store virtual machine swap files with the virtual machine configuration file, or on a local swap file datastore specified for that host.

The location of the virtual machine swap file affects vMotion compatibility as follows:

- For migrations between hosts running ESXi 6.5 and later, vMotion and migrations of suspended and powered-off virtual machines are allowed.
- During a migration with vMotion, if the swap file location on the destination host differs from the swap file location on the source host, the swap file is copied to the new location. This activity can result in slower migrations with vMotion. If the destination host cannot access the specified swap file location, it stores the swap file with the virtual machine configuration file.

See the *vSphere Resource Management* documentation for information about configuring swap file policies.

Migration with vMotion in Environments Without Shared Storage

You can use vMotion to migrate virtual machines to a different compute resource and storage simultaneously. Unlike Storage vMotion, which requires a single host to have access to both the source and destination datastore, you can migrate virtual machines across storage accessibility boundaries.

vMotion does not require environments with shared storage. This is useful for performing cross-cluster migrations, when the target cluster machines might not have access to the storage of the source cluster. Processes that are working on the virtual machine continue to run during the migration with vMotion.

You can use vMotion to migrate virtual machines across vCenter Server instances.

You can place the virtual machine and all its disks in a single location or select separate locations for the virtual machine configuration file and each virtual disk. In addition, you can change virtual disks from thick-provisioned to thin-provisioned or from thin-provisioned to thick-provisioned. For virtual compatibility mode RDMs, you can migrate the mapping file or convert from RDM to VMDK.

vMotion without shared storage is useful for virtual infrastructure administration tasks similar to vMotion with shared storage or Storage vMotion tasks.

- Host maintenance. You can move virtual machines from a host to allow maintenance of the host.
- Storage maintenance and reconfiguration. You can move virtual machines from a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.
- Storage load redistribution. You can manually redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Requirements and Limitations for vMotion Without Shared Storage

A virtual machine and its host must meet resource and configuration requirements for the virtual machine files and disks to be migrated with vMotion in the absence of shared storage.

vMotion in an environment without shared storage is subject to the following requirements and limitations:

- The hosts must be licensed for vMotion.
- The hosts must be running ESXi 5.1 or later.
- The hosts must meet the networking requirement for vMotion. See vSphere vMotion Networking Requirements.
- The virtual machines must be properly configured for vMotion. See Virtual Machine Conditions and Limitations for vMotion

- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). See Storage vMotion Requirements and Limitations.
- The destination host must have access to the destination storage.
- When you move a virtual machine with RDMs and do not convert those RDMs to VMDKs, the destination host must have access to the RDM LUNs.
- Consider the limits for simultaneous migrations when you perform a vMotion migration without shared storage. This type of vMotion counts against the limits for both vMotion and Storage vMotion, so it consumes both a network resource and 16 datastore resources. See Limits on Simultaneous Migrations.

Migration Between vCenter Server Systems

vSphere 6.0 or later lets you migrate virtual machines between vCenter Server instances.

Migration of virtual machines across vCenter Server systems is helpful in certain VM provisioning cases.

- Balance workloads across clusters and vCenter Server instances.
- Elastically expand or shrink capacity across resources in different vCenter Server instances in the same site or in another geographical area .
- Move virtual machines between environments that have different purposes, for example, from a development to production.
- Move virtual machines to meet different Service Level Agreements (SLAs) regarding storage space, performance, and so on.

Note: During the migration of a virtual machine to another vCenter Server system, the performance data that has been collected about the virtual machine is lost.

Requirements for vMotion Between vCenter Server Instances

You can use vMotion across vCenter Server instances if your system meets certain requirements.

The following list sums the requirements that your system must meet so that you can use migration across vCenter Server instances:

- When you migrate virtual machines across vCenter Server instances in Enhanced Linked Mode, without using Advanced Cross vCenter vMotion, verify that you meet the following requirements.
  - Both vCenter Server instances must be in the same vCenter Single Sign-On domain. Enhanced Link Mode lets the source vCenter Server authenticate to the destination vCenter Server.

    For information about installing vCenter Server in Enhanced Linked Mode, see the *vCenter Server Installation and Setup* documentation.
  - The cross vCenter Server and long-distance vSphere vMotion features require a vSphere Enterprise Plus license.
  - The source and destination vCenter Server instances and ESXi hosts must be 6.0 or later.
  - Both vCenter Server instances must be time-synchronized with each other for correct vCenter Single Sign-On token verification.
  - For migration of compute resources only, both vCenter Server instances must be connected to the shared virtual machine storage.

- When you migrate virtual machines across vCenter Server instances in different vCenter Single Sign-On domains with Advanced Cross vCenter vMotion, verify that you meet the following requirements.
  - The vCenter Server instance from which you initiate the import or export of virtual machines must be version 7.0 Update 1c or later.
  - To vMotion powered-on virtual machines with the Advanced Cross vCenter vMotion feature, you must have a vSphere Enterprise Plus license.
  - To migrate powered-off virtual machines with the Advanced Cross vCenter vMotion feature, you must have a vSphere Standard license.

Related Links

Network Compatibility Checks During vMotion Between vCenter Server Instances on page 1811
Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

MAC Address Management During Migration Between vCenter Server Systems on page 1812
When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1812
With Advanced Cross vCenter vMotion, you can move or clone workloads across vCenter Server systems. You can initiate migration of workloads both from on-premises environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1816
With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Network Compatibility Checks During vMotion Between vCenter Server Instances

Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

vCenter Server performs network compatibility checks to prevent the following configuration problems:

- MAC address compatibility on the destination host
- vMotion from a distributed switch to a standard switch
- vMotion between distributed switches of different versions
- vMotion to an internal network, for example, a network without a physical NIC
- vMotion to a distributed switch that is not working properly

vCenter Server does not perform checks for and notify you about the following problems:

- If the source and destination distributed switches are not in the same broadcast domain, virtual machines lose network connectivity after migration.
- If the source and destination distributed switches do not have the same services configured, virtual machines might lose network connectivity after migration.

Related Links

Requirements for vMotion Between vCenter Server Instances on page 1810
You can use vMotion across vCenter Server instances if your system meets certain requirements.

MAC Address Management During Migration Between vCenter Server Systems on page 1812

When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1812
With Advanced Cross vCenter vMotion, you can move or clone workloads across vCenter Server systems. You can initiate migration of workloads both from on-premises environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1816
With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

MAC Address Management During Migration Between vCenter Server Systems

When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

In an environment with multiple vCenter Server instances, when a virtual machine is migrated, its MAC addresses are transferred to the target vCenter Server. The source vCenter Server adds the MAC addresses to a denylist so that it does not assign them to newly created virtual machines.

To reclaim unused MAC addresses from the denylist, contact VMware Technical Support for assistance.

Related Links

Requirements for vMotion Between vCenter Server Instances on page 1810
You can use vMotion across vCenter Server instances if your system meets certain requirements.

Network Compatibility Checks During vMotion Between vCenter Server Instances on page 1811
Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1812
With Advanced Cross vCenter vMotion, you can move or clone workloads across vCenter Server systems. You can initiate migration of workloads both from on-premises environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1816
With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion

With Advanced Cross vCenter vMotion, you can move or clone workloads across vCenter Server systems. You can initiate migration of workloads both from on-premises environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

- Obtain the credentials for the administrator accounts of the vCenter Server instances to which you want to migrate virtual machines.

- Verify that the target vCenter Server instances to which you export or clone virtual machines are version 6.5 or later.
- Verify that the source vCenter Server instance from which you export virtual machines is version 7.0 Update 1c or later if you want to export virtual machines to other vCenter Server instances.
- Verify that the source vCenter Server instance from which you clone virtual machines is version 7.0 Update 3 or later.
- Verify that the destination ESXi hosts are version 6.5 or later.
- If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, verify that the destination host or cluster have available PMem resources.
- If you migrate a virtual machine that has an NVDIMM device or a vPMem disk, verify that the destination host has the proper license.
- Required privilege: **Resource.Query vMotion**
- When you migrate powered on virtual machines, verify that you meet the following requirements.
  - Required privilege: **Resource.Migrate powered on virtual machine**
  - Verify that your hosts and virtual machines meet the requirements for migration with vMotion. See Host Configuration for vMotion and Virtual Machine Conditions and Limitations for vMotion.
  - Verify that your hosts and virtual machines meet the requirements for live migration. See Requirements and Limitations for vMotion Without Shared Storage.
- When you migrate powered off virtual machines, verify that you meet the following requirements.
  - Required privilege: **Resource.Migrate powered off virtual machine**
  - Make sure that you are familiar with the requirements for cold migration. See Cold Migration.
- Required ports:
  - Port 8000 on the ESXi host for vMotion.
  - Port 902 on the ESXi host for NFC.
  - Port 443 between the two vCenter Server instances.

  For the list of all supported ports and protocols in VMware products, see the VMware Ports and Protocols Tool™ at https://ports.broadcom.com/.

With Advanced Cross vCenter vMotion, you can migrate virtual machines to a vCenter Server instance in a different vCenter Single Sign-On domain. For example, when you deploy a new vCenter Server instance, you can migrate virtual machines from the earlier version of your vCenter Server instance to the newly provisioned one.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. From the inventory tree, select the host or cluster that contains the virtual machines you want to migrate.
3. On the **VMs** tab, click the **Virtual Machines** button.
4. From the virtual machines list, select the virtual machines you want to migrate.
5. Right-click the selection and click **Migrate**.
6. If a confirmation dialog box appears, click **Yes**.

   The migration wizard appears.
7. Select **Cross vCenter Server export** as the migration type.
   a) Optional: To create a clone of the virtual machine on the target vCenter Server, select the **Keep VMs on the source vCenter Server (performs a VM clone operation).** check box.
   b) Click **Next** to continue.
8. Select the target vCenter Server instance to which you want to export or clone virtual machines.

Option	Action
Saved vCenter Servers	From the drop-down menu, select the IP address or FQDN of a saved vCenter Server.
New vCenter Server	1. Enter the IP address or FQDN, user name, and password of a vCenter Server instance.

Option	Action
	Note: The check box **Save vCenter Server address** is selected by default. If you do not want to save the vCenter Server address, deselect the check box. 2. Click **Login**.

The connection to a saved vCenter Server instance is valid only for the current user session. You must enter the credentials of the target vCenter Server instances for each login session.

9. If a **Security Alert** dialog box appears, click **Yes**.
10. Click **Next** to continue.
11. Select the destination compute resource for this virtual machine migration and click **Next**.

    Possible targets include hosts and DRS clusters with any level of automation. If DRS is not enabled for a cluster, select a specific host in the cluster rather than selecting the cluster.

    Important:

    If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

    Important: When you try to migrate a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license, the operation fails and the virtual machine is in an unmanageable state for 90 seconds. After 90 seconds, you can retry the migration, and select a destination host that is licensed to use PMem devices.
12. If a compatibility problem appears in the Compatibility pane, fix the problem or select another host or cluster for the migration.
13. Select the destination storage for the virtual machine migration.
    a) Select the storage type for the virtual machine configuration files and all the hard disks.

Mode	Description
Standard	All virtual disks are stored on a standard datastore.
PMem	All virtual disks are stored on the local PMem datastore of the host. Configuration files cannot be stored on a PMem datastore. You must additionally select a regular datastore for the configuration files of the virtual machine.
Hybrid	All PMem virtual disks remain stored on a PMem datastore. Your choice of a VM storage policy and your choice of a datastore affects non-PMem disks.

You can select the type of storage only if PMem or Hybrid storage types are available in the data center.

b) Select the format for the virtual machine disks.

c) Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important: If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

d) Select the datastore location for the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore from the list and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Configure per disk**. **Note:** You can use the **Configure per disk** option to downgrade from or upgrade to PMem storage. 2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or a Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

14. If a compatibility problem appears in the Compatibility pane, fix the problem or select another destination storage for the migration.

15. Select the destination folder for the virtual machine migration and click **Next**.

16. Select the destination networks for the virtual machine migration.

Option	Action
Select a destination network for all VM network adapters connected to a valid source network.	1. Click the arrow in the **Destination Network** column and select **Browse**. 2. Select a destination network and click **OK**. 3. Click **Next**.
Select a different destination network for each VM network adapter connected to a valid source network.	1. Click **Advanced**. 2. Click the arrow in the **Destination Network** column and select **Browse**. 3. Select a destination network and click **OK**. 4. Click **Next**.

17. On the **Ready to complete** page, review the details and click **Finish**.

The virtual machines are moved or cloned to the destination folder in the new vCenter Server instance. You can monitor the migration process in the **Recent tasks** pane. If errors occur during the migration, the virtual machines revert to their original states and locations.

Related Links

Requirements for vMotion Between vCenter Server Instances on page 1810
You can use vMotion across vCenter Server instances if your system meets certain requirements.

Network Compatibility Checks During vMotion Between vCenter Server Instances on page 1811
Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

MAC Address Management During Migration Between vCenter Server Systems on page 1812
When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1816
With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Import or Clone a Virtual Machine with Advanced Cross vCenter vMotion

With Advanced Cross vCenter vMotion, you can migrate workloads across vCenter Server systems. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

- Obtain the credentials for the administrator account of the vCenter Server instance from which you want to import or clone virtual machines.
- Verify that the source vCenter Server instances from which you import or clone virtual machines are version 6.5 or later.
- Verify that the target vCenter Server instance to which you import virtual machines is version 7.0 Update 1c or later.
- Verify that the target vCenter Server instance to which you clone virtual machines is version 7.0 Update 1c or later.
- Verify that the destination ESXi hosts are version 6.5 or later.
- If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, verify that the destination host or cluster have available PMem resources.
- If you migrate a virtual machine that has an NVDIMM device or a vPMem disk, verify that the destination host has the proper license.
- Required privilege: **Resource.Query vMotion**
- When you migrate powered on virtual machines, verify that you meet the following requirements.
  - Required privilege: **Resource.Migrate powered on virtual machine**
  - Verify that your hosts and virtual machines meet the requirements for migration with vMotion. See Host Configuration for vMotion and Virtual Machine Conditions and Limitations for vMotion.
  - Verify that your hosts and virtual machines meet the requirements for live migration. See Requirements and Limitations for vMotion Without Shared Storage.
- When you migrate powered off virtual machines, verify that you meet the following requirements.
  - Required privilege: **Resource.Migrate powered off virtual machine**
  - Make sure that you are familiar with the requirements for cold migration. See Cold Migration.

- Required ports:
  - Port 8000 on the ESXi host for vMotion.
  - Port 902 on the ESXi host for NFC.
  - Port 443 between the two vCenter Server instances.

  For the list of all supported ports and protocols in VMware products, see the VMware Ports and Protocols Tool™ at https://ports.broadcom.com/.

With Advanced Cross vCenter vMotion, you can import or clone virtual machines from a vCenter Server instance in a different vCenter Single Sign-On domain. For example, when you deploy a new vCenter Server instance, you can migrate virtual machines from the earlier version of your vCenter Server instance to the newly provisioned one.

1. In the vSphere Client home page, navigate to **Home** > **Hosts and Clusters**.
2. From the inventory tree, right-click the host or cluster to which you want to import virtual machines.
3. Click **Import VMs**.

   The **Import VMs** wizard appears.
4. Select the source vCenter Server instance from which you want to import virtual machines.

Option	Action
Saved vCenter Servers	From the drop-down menu, select the IP address or FQDN of a saved vCenter Server instance.
New vCenter Server	1. Enter the IP address or FQDN, user name, and password of a vCenter Server instance. **Note:** The check box **Save vCenter Server address** is selected by default. If you do not want to save the vCenter Server address, deselect the check box. 2. Click **Login**.

   The connection to a saved vCenter Server instances is valid only for the current user session. You must enter the credentials of the source vCenter Server instances for each login session.
5. If a **Security Alert** dialog box appears, click **Yes**.
6. Click **Next**.
7. Select the virtual machines to import or clone.
   a) If you want to migrate more than one virtual machine, the selected virtual machines must be in the same power state.
   b) To keep a clone of the virtual machine on the source vCenter Server, select the **Keep VMs on the source vCenter Server (performs a VM clone operation).** check box.
   c) Click **Next** to continue.

   If you want to migrate more than one virtual machine, the selected virtual machines must be in the same power state.
8. Select the destination compute resource for this virtual machine migration and click **Next**.

   Possible targets include hosts and DRS clusters with any level of automation. If DRS is not enabled for a cluster, select a specific host in the cluster rather than selecting the cluster.

   Important:

   If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore.

Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important: When you try to migrate a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license, the operation fails and the virtual machine is in an unmanageable state for 90 seconds. After 90 seconds, you can retry the migration, and select a destination host that is licensed to use PMem devices.

9. If a compatibility problem appears in the Compatibility pane, fix the problem or select another host or cluster for the migration.
10. Select the destination storage for the virtual machine migration.
    a) Select the storage type for the virtual machine configuration files and all the hard disks.

Mode	Description
Standard	All virtual disks are stored on a standard datastore.
PMem	All virtual disks are stored on the local PMem datastore of the host. Configuration files cannot be stored on a PMem datastore. You must additionally select a regular datastore for the configuration files of the virtual machine.
Hybrid	All PMem virtual disks remain stored on a PMem datastore. Your choice of a VM storage policy and your choice of a datastore affects non-PMem disks.

    You can select the type of storage only if PMem or Hybrid storage types are available in the data center.
    b) Select the format for the virtual machine disks.
    c) Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

    Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

    Important: If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.
    d) Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore from the list and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Configure per disk**. **Note:** You can use the **Configure per disk** option to downgrade from or upgrade to PMem storage.

Option	Action
	2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you want to migrate the virtual machine to a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

11. If a compatibility problem appears in the Compatibility pane, fix the problem or select another destination storage for the migration.
12. Select the destination folder for the virtual machines and click **Next**.
13. Select the destination networks for the virtual machine migration.

Option	Action
Select a destination network for all VM network adapters connected to a valid source network.	1. Click the arrow in the **Destination Network** column and select **Browse**. 2. Select a destination network and click **OK**. 3. Click **Next**.
Select a different destination network for each VM network adapter connected to a valid source network.	1. Click **Advanced**. 2. Click the arrow in the **Destination Network** column and select **Browse**. 3. Select a destination network and click **OK**. 4. Click **Next**.

14. On the **Ready to complete** page, review the details and click **Finish**.

The virtual machines are moved or cloned to the destination folder in the current vCenter Server instance. You can monitor the migration process in the **Recent tasks** pane. If errors occur during the migration, the virtual machines revert to their original states and locations.

Related Links

Requirements for vMotion Between vCenter Server Instances on page 1810
You can use vMotion across vCenter Server instances if your system meets certain requirements.

Network Compatibility Checks During vMotion Between vCenter Server Instances on page 1811
Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

MAC Address Management During Migration Between vCenter Server Systems on page 1812
When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

Export or Clone a Virtual Machine with Advanced Cross vCenter vMotion on page 1812
With Advanced Cross vCenter vMotion, you can move or clone workloads across vCenter Server systems. You can initiate migration of workloads both from on-premises environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Migration with Storage vMotion

With Storage vMotion, you can migrate a virtual machine and its disk files from one datastore to another while the virtual machine is running. With Storage vMotion, you can move virtual machines off of arrays for maintenance or to upgrade. You also have the flexibility to optimize disks for performance, or to transform disk types, which you can use to reclaim space.

You can choose to place the virtual machine and all its disks in a single location, or you can select separate locations for the virtual machine configuration file and each virtual disk. The virtual machine does not change execution host during a migration with Storage vMotion.

During a migration with Storage vMotion, you can change the disk provisioning type.

Migration with Storage vMotion changes virtual machine files on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and `.nvram` files. If the new names exceed the maximum filename length, the migration does not succeed.

Storage vMotion has several uses in administering virtual infrastructure, including the following examples of use.

- Storage maintenance and reconfiguration. You can use Storage vMotion to move virtual machines off a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.
- Redistributing storage load. You can use Storage vMotion to redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Storage vMotion Requirements and Limitations

A virtual machine and its host must meet resource and configuration requirements for the virtual machine disks to be migrated with Storage vMotion.

Storage vMotion is subject to the following requirements and limitations:

- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). For virtual compatibility mode RDMs, you can migrate the mapping file or convert to thick-provisioned or thin-provisioned disks during migration if the destination is not an NFS datastore. If you convert the mapping file, a new virtual disk is created and the contents of the mapped LUN are copied to this disk. For physical compatibility mode RDMs, you can migrate the mapping file only.
- Migration of virtual machines during VMware Tools installation is not supported.
- Because VMFS3 datastores do not support large capacity virtual disks, you cannot move virtual disks greater than 2 TB from a VMFS5 datastore to a VMFS3 datastore.
- The host on which the virtual machine is running must have a license that includes Storage vMotion.
- ESXi 4.0 and later hosts do not require vMotion configuration to perform migration with Storage vMotion.
- The host on which the virtual machine is running must have access to both the source and target datastores.
- For limits on the number of simultaneous migrations with vMotion and Storage vMotion, see Limits on Simultaneous Migrations.

CPU Compatibility and EVC

vCenter Server performs compatibility checks before it allows migration of running or suspended virtual machines to ensure that the virtual machine is compatible with the target host.

vMotion transfers the running state of a virtual machine between underlying ESXi systems. Live migration requires that the processors of the target host provide the same instructions to the virtual machine after migration that the processors of the source host provided before migration. Clock speed, cache size, and number of cores can differ between source and target processors. However, the processors must come from the same vendor class (AMD or Intel) to be vMotion compatible.

Migrations of suspended virtual machines also require that the virtual machine be able to resume execution on the target host using equivalent instructions.

When you initiate a migration with vMotion or a migration of a suspended virtual machine, the **Migrate Virtual Machine** wizard checks the destination host for compatibility. If compatibility problems prevent migration, the wizard displays an error message.

The CPU instruction set available to the operating system and to applications running in a virtual machine is determined at the time that a virtual machine is powered on. This CPU feature set is based on the following items:

- Host CPU family and model
- Settings in the BIOS that might deactivate CPU features
- ESXi version running on the host
- The compatibility setting of the virtual machine
- The guest operating system of the virtual machine

To improve CPU compatibility between hosts of varying CPU feature sets, some host CPU features can be hidden from the virtual machine by placing the host in an Enhanced vMotion Compatibility (EVC) cluster. For more information about EVC, see About Enhanced vMotion Compatibility.

Note:

You can hide Host CPU features from a virtual machine by applying a custom CPU compatibility mask to the virtual machine, but this is not recommended. VMware, in partnership with CPU and hardware vendors, is working to maintain vMotion compatibility across the widest range of processors. For additional information, search the VMware Knowledge Base for the *vMotion and CPU Compatibility FAQ*.

CPU Compatibility Scenarios

vCenter Server's CPU compatibility checks compare the CPU features available on the source host, the subset of features that the virtual machine can access, and the features available on the target host. Without the use of EVC, any mismatch between user-level features of the hosts blocks migration, whether or not the virtual machine itself has access to those features. A mismatch between kernel-level features of the hosts blocks migration only when the virtual machine has access to a feature that the target host does not provide.

User-level features are non-privileged instructions used by virtual machine applications. These include SSE3, SSSE3, SSE4.1, SSE4.2, and AES. Because they are user-level instructions that bypass the virtualization layer, these instructions can cause application instability if mismatched after a migration with vMotion.

Kernel-level features are privileged instructions used by the virtual machine operating system. These include the AMD No eXecute (NX) and the Intel eXecute Disable (XD) security features.

When you attempt to migrate a virtual machine with vMotion, one of the following scenarios applies:

- The destination host feature set matches the CPU feature set of the virtual machine. CPU compatibility requirements are met, and migration with vMotion proceeds.
- The CPU feature set of the virtual machine contains features not supported by the destination host. CPU compatibility requirements are not met, and migration with vMotion cannot proceed.
  Note: EVC overcomes such incompatibility by providing a "baseline" feature set for all virtual machines running in a cluster. This baseline feature set hides the differences among the clustered hosts' CPUs from the virtual machines.
- The destination host supports the feature set of the virtual machine, plus additional user-level features (such as SSE4.1) not found in the feature set of the virtual machine. CPU compatibility requirements are not met, and migration with vMotion cannot proceed.
  Note: This type of incompatibility is ignored for migrations among hosts in EVC clusters.
- The destination host supports the feature set of the virtual machine, plus additional kernel-level features (such as NX or XD) not found in the feature set of the virtual machine. CPU compatibility requirements are met, and migration with vMotion proceeds. The virtual machine retains its CPU feature set while it remains powered on, allowing it to migrate

freely back to the original host. However, if the virtual machine is rebooted, it acquires a new feature set from the new host. This process might cause vMotion incompatibility if you attempt to migrate the virtual machine back to the original host.

CPU Families and Feature Sets

Processors are grouped into families. Processors within a given family generally have similar feature sets.

Processor vendors define processor families. You can distinguish different processor versions within the same family by comparing the processors' model, stepping level, and extended features. Sometimes, processor vendors have introduced significant architectural changes within the same processor family, such as the SSSE3 and SSE4.1 instructions, and NX/XD CPU security features.

By default, vCenter Server identifies mismatches on features accessible to applications as incompatible to guarantee the stability of virtual machines after migrations with vMotion.

Server hardware's CPU specifications usually indicate whether or not the CPUs contain the features that affect vMotion compatibility.

For more information on identifying Intel processors and their features, see *Application Note 485: Intel® Processor Identification and the CPUID Instruction*, available from Intel. For more information on identifying AMD processors and their features, see *CPUID Specification*, available from AMD.

About Enhanced vMotion Compatibility

You can use the Enhanced vMotion Compatibility (EVC) feature to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. Using EVC prevents migrations with vMotion from failing because of incompatible CPUs.

Configure EVC from the cluster settings dialog box. When you configure EVC, you configure all host processors in the cluster to present the feature set of a baseline processor. This baseline feature set is called the EVC mode. EVC uses AMD-V Extended Migration technology (for AMD hosts) and Intel FlexMigration technology (for Intel hosts) to mask processor features so that hosts can present the feature set of an earlier generation of processors. The EVC mode must be equivalent to, or a subset of, the feature set of the host with the smallest feature set in the cluster.

EVC masks only those processor features that affect vMotion compatibility. Enabling EVC does not prevent a virtual machine from taking advantage of faster processor speeds, increased numbers of CPU cores, or hardware virtualization support that might be available on newer hosts.

EVC cannot prevent virtual machines from accessing hidden CPU features in all circumstances. Applications that do not follow CPU vendor recommended methods of feature detection might behave unexpectedly in an EVC environment. VMware EVC cannot be supported with ill-behaved applications that do not follow the CPU vendor recommendations. For more information about creating well-behaved applications, search the VMware Knowledge Base for the article *Detecting and Using New Features in CPUs*.

Starting with vSphere 7.0 Update 1, you can take advantage of the EVC feature for Virtual Shared Graphics Acceleration (vSGA). vSGA allows multiple virtual machines to share GPUs installed on ESXi hosts and leverage the 3D graphics acceleration capabilities.

EVC Requirements for Hosts

To improve CPU compatibility between hosts that have varying CPU feature sets, you can hide some host CPU features from the virtual machines by placing the host in an Enhanced vMotion Compatibility (EVC) cluster. Hosts in an EVC cluster and hosts that you add to an existing EVC cluster must meet EVC requirements.

- Power off all virtual machines in the cluster that are running on hosts with a feature set greater than the EVC mode that you intend to enable. You can also migrate these virtual machines out of the cluster.
- All hosts in the cluster must meet the following requirements:

Requirements	Description
Supported ESXi version	ESXi 6.5 or later.
vCenter Server	The host must be connected to a vCenter Server system.
CPUs	A single vendor, either AMD or Intel.
Advanced CPU features enabled	Enable these CPU features in the BIOS if they are available: • Hardware virtualization support (AMD-V or Intel VT) • AMD No eXecute(NX) • Intel eXecute Disable (XD) **Note:** Hardware vendors sometimes deactivate particular CPU features in the BIOS by default. You might have problems enabling EVC because the EVC compatibility checks detect the absence of features that are expected to be present for a particular CPU. If you cannot enable EVC on a system with a compatible processor, ensure that all features are enabled in the BIOS.
Supported CPUs for the EVC mode that you want to enable	To check EVC support for a specific processor or server model, see the *Broadcom Compatibility Guide* at https://compatibilityguide.broadcom.com/.
Configured for vMotion	See Host Configuration for vMotion.

Enable EVC on an Existing Cluster

Enable EVC on an existing cluster to ensure vMotion CPU compatibility between the hosts in the cluster. Other cluster features such as vSphere DRS and vSphere HA are fully compatible with EVC.

Verify that the hosts in the cluster meet the requirements listed in EVC Requirements for Hosts.

1. Select a cluster in the vSphere inventory.
2. Power off all the virtual machines on the hosts with feature sets greater than the EVC mode.

   To determine the EVC mode of all virtual machines on the hosts in the cluster, see Determine the EVC Mode of a Virtual Machine. You must power off all powered on virtual machine with no EVC mode or with an EVC mode that is greater than the EVC mode that you plan to enable on the cluster.
3. Click the **Configure** tab, select VMware EVC, and click **Edit**.
4. Enable EVC for the CPU vendor and feature set appropriate for the hosts in the cluster, and click **OK**.
5. Power on the virtual machines in the cluster to apply the EVC.

Change the EVC Mode for a Cluster

Configure EVC to ensure that virtual machine migrations between hosts in the cluster do not fail because of CPU feature incompatibilities.

- Verify that all hosts in the cluster have supported CPUs for the EVC mode you want to enable. See Knowledge Base article KB 1003212 for a list of supported CPUs.

- Verify that all hosts in the cluster are connected and registered on vCenter Server. The cluster cannot contain a disconnected host.
- Virtual machines must be in the following power states, depending on whether you raise or lower the EVC mode.

EVC Mode	Virtual Machine Power Action
Raise the EVC mode to a CPU baseline with more features.	Running virtual machines can remain powered on. New EVC mode features are not available to the virtual machines until they are powered off and powered back on again. A full power cycling is required. Rebooting the guest operating system or suspending and resuming the virtual machine is not sufficient. **Tip:** You can configure a virtual machine to power cycle when its guest OS is rebooted, by setting the `vmx.reboot.powerCycle` VM parameter to `TRUE`. When the virtual machine is powered back on, this configuration parameter is removed. To edit the virtual machine configuration settings, you can use the VMware Host Client. See *Edit the Configuration File Parameters in the VMware Host Client* topic in the *vSphere Single Host Management - VMware Host Client* guide. See the VMware vSphere Blog post for information about how to set this parameter to a group of virtual machines using VMware PowerCLI.
Lower the EVC mode to a CPU baseline with fewer features.	Power off virtual machines if they are powered on and running at a higher EVC mode than the one you intend to enable.

Note: When you take a snapshot of a virtual machine in an EVC cluster, keep in mind the following use cases:

- If you take a snapshot of a running virtual machine before an EVC downgrade, an attempt to revert to that snapshot after the EVC downgrade fails and the virtual machine is left in a suspended state.
- If you take a snapshot of a virtual machine before an EVC upgrade, you can revert to that snapshot before or after the EVC upgrade.

To verify the EVC mode for virtual machines, see Determine the EVC Mode of a Virtual Machine.

Several EVC approaches are available to ensure CPU compatibility:

- If all the hosts in a cluster are compatible with a newer EVC CPU or Graphics (vSGA) mode, you can change the EVC CPU or Graphics (vSGA) mode of an existing EVC cluster.
- You can enable EVC for a cluster that does not have EVC enabled.
- You can raise the EVC mode to expose more CPU features.
- You can lower the EVC mode to hide CPU features and increase compatibility.

1. Select a cluster in the inventory.
2. Click the **Configure** tab.
3. Under **Configuration**, select **VMware EVC**, and click **Edit**.
4. On the **Change EVC Mode** page, select whether to activate or deactivate EVC.

Option	Description
Disable EVC	The EVC feature is deactivated. CPU compatibility is not enforced for the hosts in this cluster.
Enable EVC for AMD Hosts	The EVC feature is activated for AMD hosts.
Enable EVC for Intel Hosts	The EVC feature is activated for Intel hosts.

5. From the **CPU Mode** drop-down menu, select the baseline CPU feature set that you want to activate for the cluster.

   If you cannot select the EVC CPU Mode, the Compatibility pane displays the reason, and the relevant hosts for each reason.

6. Optional: From the **Graphics Mode (vSGA)** drop-down menu, select a baseline graphics feature set.

   If you cannot select the EVC vSGA Mode, the Compatibility pane displays the reason, and the relevant hosts for each reason.

Option	Description
Baseline Graphics	Applies the Baseline Graphics feature set that includes features through Direct3D 10.1/OpenGL 3.3. **Note: Graphics Mode (vSGA)** applies only the Baseline Graphics set that includes features through Direct3D 10.1/ OpenGL 3.3. The Baseline Graphics feature set is compatible with all supported features for ESXi 6.5 or later.
D3D 11.0 class features	Applies the baseline graphics feature set that includes features through Direct3D 11.0/OpenGL 4.1. **Note:** When you create a cluster, if you enable EVC graphics mode D3D 11.0 class features, you can add only ESXi hosts that support Direct3D 11.0 to the cluster. When you try to add an ESXi host that does not support Direct3D 11.0 to the cluster, the operation fails with an error message.

7. Click **OK**.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU and graphics features that a host must have in order for the virtual machine to migrate to that host and power on. The EVC mode of a virtual machine is independent from the EVC mode that you configure for the cluster in which the virtual machine runs.

The EVC mode of a virtual machine is determined when the virtual machine powers on. At power-on, the virtual machine also determines the EVC mode of the cluster in which it runs. If the EVC mode of a running virtual machine or the entire EVC cluster is raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not use any CPU features exposed by the new EVC mode until the virtual machine is powered off and powered on again.

For example, you create an EVC cluster that contains hosts with Intel processors and you set the EVC mode to Intel "Merom" Generation (Xeon Core 2). When you power on a virtual machine in this cluster, it runs in the Intel Merom Generation (Xeon Core 2) EVC mode. If you raise the EVC mode of the cluster to Intel "Penryn" Generation (Xeon 45 nm Core 2), the virtual machine retains the lower Intel "Merom" Generation (Xeon Core 2) EVC mode. To use the feature set of the higher EVC mode, such as SSE4.1, the virtual machine must be powered off and powered on again.

1. Navigate to a cluster or a host in the vCenter Server inventory.
2. Click the **VMs** > **Virtual Machines** tab.

   A list of all virtual machines in the selected cluster or on the selected host appears.

3. To verify the status of the CPU mode, check the **EVC CPU Mode** column.
   a) If the column is not visible, click the **Pick columns** icon ( ) at the bottom left corner of the **Virtual Machines** table.

      The **Show Columns** pop-up appears.
   b) To show the **EVC CPU Mode** column, locate and select the respective check box from the list.

   The **EVC CPU Mode** column shows the CPU modes of all virtual machines in the cluster or on the host.

   Important: For each virtual machine, the **EVC CPU Mode** column displays the EVC mode defined at the virtual machine level.

   However, if you do not configure per-VM EVC for a virtual machine, the virtual machine inherits the EVC mode of its parent cluster or host. As a result, for all virtual machines that do not have per-VM EVC configured, the **EVC CPU Mode** column displays the inherited EVC mode of the parent host or cluster.

   If the virtual machine is in an EVC cluster, the EVC mode that you see in the **EVC CPU Mode** column is defined in the following manner.

   - When the virtual machine is powered on, the **EVC CPU Mode** column displays either the per-VM EVC mode, or the cluster-level EVC mode.

Per-VM EVC	Cluster-Level EVC	EVC Mode for the Virtual Machine
Activated	Activated	Enabled. The **EVC CPU Mode** column displays the EVC mode of the virtual machine.
Deactivated	Activated	Enabled. The **EVC CPU Mode** column displays the EVC mode of the EVC cluster.

   - When the virtual machine is powered off, the **EVC CPU Mode** column displays the per-VM EVC mode. If per-VM EVC is disabled, the **EVC CPU Mode** column for the virtual machine is empty.

   When the virtual machine is not in an EVC cluster and per-VM EVC is not configured, the EVC mode that you see in the **EVC CPU Mode** column is defined in the following manner.

   - When the virtual machine is powered on, the **EVC CPU Mode** column displays the EVC mode of the parent host.
   - When the virtual machine is powered off, the **EVC CPU Mode** column is empty.

4. To verify the status of the graphics mode, check the **EVC Graphics Mode (vSGA)** column.
   a) If the column is not visible, click the **Pick columns** icon ( ) at the bottom left corner of the **Virtual Machines** table.

      The **Show Columns** pop-up appears.
   b) To show the **EVC Graphics Mode (vSGA)** column, locate and select the respective check box from the list.

   The **EVC Graphics Mode (vSGA)** column displays the baseline graphics features set. To view the baseline graphics, you must enable **3D graphics** in the virtual machine.

   For information about configuring 3D graphics in a virtual machine, see the *vSphere Virtual Machine Administration* guide.

Determine the EVC Mode that a Host Supports

By determining the EVC modes that the host can support, you can determine whether the host is compatible with other hosts in an EVC cluster. For hosts to be included in the same EVC cluster, all the hosts must support at least one common mode.

1. Select a host in the inventory.
2. Click the **Summary** tab.
3. In the Configuration panel, expand **EVC Mode**.
   The supported EVC modes are listed in order from the fewest to the greatest number of supported features.

Prepare Clusters for AMD Processors Without 3DNow!

Newer generations of AMD processors do not include 3DNow! processor instructions. If hosts in a cluster have different generations of AMD processors, some with 3DNow! instruction sets and some without, you cannot successfully migrate virtual machines between the hosts. You must use an EVC mode or CPU compatibility mask to hide the instructions.

Ensure that the cluster contains only hosts with AMD Opteron Generation 3 or newer processors.

The vCenter Server**AMD Opteron Gen. 3 (no 3DNow!)** EVC mode masks the 3DNow! instructions from virtual machines. You can apply this EVC mode to EVC clusters containing only AMD Opteron Generation 3 hosts. Applying this mode allows the clusters to maintain vMotion compatibility with AMD Opteron hosts that do not have 3DNow! instructions. Clusters containing AMD Opteron Generation 1 or AMD Opteron Generation 2 hosts cannot be made vMotion-compatible with hosts that do not have 3DNow! instructions.

- Enable the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode for your EVC cluster.
  The steps to enable the EVC mode differ depending on whether you are creating a cluster or enabling the mode on an existing cluster, and on whether the existing cluster contains powered-on virtual machines.

Option	Description
Creating a cluster	In the New Cluster wizard, enable EVC for AMD hosts and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode.
Editing a cluster without powered-on virtual machines	In the Cluster Settings dialog box, edit the **VMware EVC** settings and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode.
Editing a cluster with powered-on virtual machines	The **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode cannot be enabled while there are powered-on virtual machines in the cluster. 1. Power-off any running virtual machines in the cluster, or migrate them out of the cluster using vMotion. Migrating the virtual machines out of the cluster with vMotion allows you to delay powering off the virtual machines until a more convenient time. 2. In the Cluster Settings dialog box, edit the **VMware EVC** settings and select the **AMD Opteron Gen. 3 (no 3DNow!)** EVC mode. 3. If you migrated virtual machines out of the cluster, power them off and cold migrate them back into the cluster. 4. Power on the virtual machines.

You can now add hosts with AMD processors without 3DNow! instructions to the cluster and preserve vMotion compatibility between the new hosts and the existing hosts in the cluster.

CPU Compatibility Masks

CPU compatibility masks allow customization of the CPU features visible to a virtual machine.

vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether or not to allow migrations with vMotion.

To guarantee the stability of virtual machines after a migration with vMotion, VMware sets the default values for CPU compatibility masks.

When a choice between CPU compatibility or guest operating system features (such as NX/XD) exists, VMware provides check-box options to configure individual virtual machines. You can access the configuration options through the Advanced Settings option for the CPU of the virtual machine. For more control over the visibility of CPU features, you can edit the CPU compatibility mask of the virtual machine at the bit level.

CAUTION: Changing the CPU compatibility masks can result in an unsupported configuration. Do not manually change the CPU compatibility masks unless instructed to do so by VMware Support or a VMware Knowledge base article.

CPU compatibility masks cannot prevent virtual machines from accessing masked CPU features in all circumstances. In some circumstances, applications can detect and use masked features even though they are hidden from the guest operating system. In addition, on any host, applications that use unsupported methods of detecting CPU features rather than using the CPUID instruction can access masked features. Virtual machines running applications that use unsupported CPU detection methods might experience stability problems after migration.

View Feature Capabilities Details for an EVC Cluster

The feature set that is exposed by an EVC cluster corresponds to the feature set of a particular type of processor. Processor feature sets are described by a set of feature flags that you examine using the CPUID instruction.

You can view the CPUID feature flags currently exposed by the hosts in an EVC cluster.

1. Select a cluster in the inventory.
2. Click the **Configure** tab.
3. Select **VMware EVC** and expand **Current Feature Capabilities Details**.

This VMware EVC panel displays the CPUID feature flags that EVC enforces for the hosts in this cluster. For information about CPUID feature flags, see the Intel and AMD websites.

Migrate a Powered Off or Suspended Virtual Machine

You can use cold migration to move a virtual machine and its associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

-
- Required privilege: **Resource** > **Migrate powered off virtual machine**

1. Power off or suspend the virtual machine.
2. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
3. Select the migration type and click **Next**.

Option	Description
Change compute resource only	Move the virtual

Option	Description
	machine to another host.
Change storage only	Move the virtual machine's configuration file and virtual disks.
Change both compute resource and storage	Move the virtual machine to another host and move its configuration file and virtual disks.

4. If you change the compute resource of the virtual machine, select the destination compute resource for this virtual machine migration and click **Next**.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and DRS clusters with any level of automation. If a cluster has no DRS enabled, select a specific host in the cluster rather than selecting the cluster.

   Important:

   If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

   If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

   Important:

   Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

5. If you change the storage of the virtual machine, enter the required details in the **Select Storage** page.
   a) Select the storage type for the virtual machine configuration files and all the hard disks.
      - If you select the **Standard** mode, all virtual disks are stored on a standard datastore.
      - If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.
      - If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

      Selecting the type of storage is possible only if PMem or Hybrid storage types are available in the data center.
   b) Select the format for the virtual machine disks.
   c) Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

      Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

      Important:

      If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.
   d) Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore from the list and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. To deactivate Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Configure per disk**. **Note:** You can use the **Configure per disk** option to downgrade from or upgrade to PMem storage. 2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

6. If you change the compute resource of the virtual machine, select destination networks for the virtual machine migration.

   You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

Option	Action
Select a destination network for all VM network adapters connected to a valid source network.	1. Click the arrow in the **Destination Network** column and select **Browse**. 2. Select a destination network and click **OK**. 3. Click **Next**.
Select a new destination network for each VM network adapter connected to a valid source network.	1. Click **Advanced**. 2. Click the arrow in the **Destination Network** column and select **Browse**. 3. Select a destination network and click **OK**. 4. Click **Next**.

7. On the **Ready to complete** page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource

You can use the **Migration** wizard to migrate a powered-on virtual machine from one compute resource to another by using vMotion. To relocate only the disks of a powered-on virtual machine, migrate the virtual machine to a new datastore by using Storage vMotion.

Verify that your hosts and virtual machines meet the requirements for migration with vMotion with shared storage.

- Required privilege: **Resource** > **Migrate powered on virtual machine**

1. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
2. Click **Change compute resource only** and click **Next**.
3. Select a host, cluster, resource pool, or vApp to run the virtual machine, and click **Next**.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and fully automated DRS clusters in the same or another vCenter Server system. If your target is a non-automated cluster, select a host within the non-automated cluster.

   Important:

   If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

   If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resources, so that all PMem hard disks remain stored on a

PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important: Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

4. Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

   You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

   You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

5. Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is

Option	Description
	not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

6. Review the page and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource and Storage

You can move a virtual machine to another compute resource and move its disks or virtual machine folder to another datastore. With vMotion, you can migrate a virtual machine and its disks and files while the virtual machine is powered on.

- Required privilege: **Resource** > **Migrate powered on virtual machine**

Simultaneous migration to a new compute resource and datastore provides greater mobility for virtual machines by eliminating the vCenter Server boundary. Virtual machine disks or contents of the virtual machine folder are transferred over the vMotion network to reach the destination host and datastores.

To make disk format changes and preserve them, you must select a different datastore for the virtual machine files and disks. You cannot preserve disk format changes if you select the same datastore on which the virtual machine currently resides.

1. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
2. Select **Change both compute resource and storage** and click **Next**.
3. Select a destination resource for the virtual machine, and click **Next**.

   Any compatibility problems appear in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and fully automated DRS clusters. If your target is a non-automated cluster, select a host within the non-automated cluster.

   If your environment has more than one vCenter Server instances, you can move virtual machines from one vCenter Server inventory to another.

   Important:

   If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

   If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

   Important:

   Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.
4. Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.

Option	Action
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports

Option	Action
	clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other

Option	Action
	types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

5. Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

   Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

   Important:

   If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

6. Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. To deactivate Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Advanced**. **Note:** You can use the **Advanced** option to downgrade from or upgrade to PMem storage. 2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

7. Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

   You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

   You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

8. Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with

Option	Description
	vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a

Option	Description
	lack of CPU resources, the duration of vMotion can be extended.

9. On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to New Storage

Use migration with Storage vMotion to relocate the configuration file of a virtual machine and its virtual disks while the virtual machine is powered on.

- Required privilege: **Resource** > **Migrate powered on virtual machine**

You can change the virtual machine host during a migration with Storage vMotion.

1. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
2. Click **Change storage only** and click **Next**.
3. Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required

Option	Action
	for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual

Option	Action
	disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first,

Option	Action
	a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

4. Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

   Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

   Important:

   If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

5. Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. To deactivate Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster.

Option	Action
	3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Advanced**. **Note:** You can use the **Advanced** option to downgrade from or upgrade to PMem storage. 2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

6. On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new storage location. Names of migrated virtual machine files on the destination datastore match the inventory name of the virtual machine.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Place vMotion Traffic on the vMotion TCP/IP Stack of an Host

Use the vMotion TCP/IP stack to isolate traffic for vMotion and to assign a dedicated default gateway, routing table, and DNS configuration for this traffic. To enable the vMotion TCP/IP stack, assign a new VMkernel adapter to it.

Verify that the host is running 6.0 or later

By using a separate TCP/IP stack, you can handle vMotion and cold migration traffic according to the topology of the network and as required for your organization:

- Route the traffic for migration of powered on or powered off virtual machines by using a default gateway. The gateway must be different from the gateway assigned to the default stack on the host.
  By using a separate default gateway, you can use DHCP for IP address assignment to the VMkernel adapters for migration in a flexible way.
- Assign a separate set of buffers and sockets.
- Avoid routing table conflicts that might otherwise appear when many features are using a common TCP/IP stack.
- Isolate traffic to improve security.

1. In the vSphere Client, navigate to the host.
2. Click the **Configure** tab.
3. Select **Networking**, and click **VMkernel adapters**.
4. Click **Add networking**.
5. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
6. On the Select target device page, select the switch for the VMkernel adapter, and click **Next**.

Option	Description
Select an existing network	Use the

Option	Description
	physical adapter configuration of an existing distributed port group to send data from the VMkernel adapter to the external network.
Select an existing standard switch	Use the physical adapter configuration for the VMkernel adapter of an existing standard switch.
New vSphere standard switch	Assign a new physical adapter configuration for the VMkernel adapter on a new standard switch.

7. On the Port properties page, select **vMotion** from the **TCP/IP stack** drop-down menu.

   The vMotion traffic becomes the only service that is enabled. You cannot use this VMkernel adapter for traffic types other than vMotion.

8. Set the label, VLAN ID, and IP mode of the VMkernel adapter, and click **Next**.

9. Optional: On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack. Select the

Option	Description
	Override default gateway for this adapter check box and enter a gateway address, if you want to specify a different gateway for the VMkernel adapter. **Note:** Selected netstack should have the default gateway explicitly on each host.

10. Optional: On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on

Option	Description
	the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisemer to obtain IPv6 addresses. In ESXi 6.5 and later router advertisemer is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	1. Click **Add IPv6 address** to add a new IPv6 address. 2. Enter the IPv6 address and subnet prefix length, and click **OK**. 3. To change

Option	Description
	the VMkerne default gateway, click **Overrid default gateway for this adapter**. The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

11. Review your settings selections on the Ready to complete page and click **Finish**.

After you create a VMkernel adapter on the vMotion TCP/IP stack, you can use only this stack for vMotion on this host. The VMkernel adapters on the default TCP/IP stack are deactivated for the vMotion service. If a live migration uses the default TCP/IP stack while you are configuring VMkernel adapters with the vMotion TCP/IP stack, the migration completes successfully. However, the involved VMkernel adapters on the default TCP/IP stack are deactivated for future vMotion sessions.

Assign a default gateway, and configure the DNS settings, congestion control, and maximum number of connections for the vMotion TCP/IP stack.

For more information on how to change the configuration of a TCP/IP stack on a host, see the *vSphere Networking* documentation.

How to Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack

Learn how to use the provisioning TCP/IP stack to isolate traffic for cold migration, VM clones, snapshots, and cold data in hot migration, and to assign a dedicated default gateway, routing table, and DNS configuration for this traffic. To enable the Provisioning TCP/IP stack, assign a new VMkernel adapter to it.

Verify that the host is running 6.0 or later

By using a separate TCP/IP stack, you can handle vMotion and cold migration traffic according to the topology of the network and as required for your organization:

- Route the traffic for migration of powered on or powered off virtual machines by using a default gateway. The gateway must be different from the gateway assigned to the default stack on the host.
  By using a separate default gateway, you can use DHCP for IP address assignment to the VMkernel adapters for migration in a flexible way.
- Assign a separate set of buffers and sockets.
- Avoid routing table conflicts that might otherwise appear when many features are using a common TCP/IP stack.
- Isolate traffic to improve security.

1. In the vSphere Client, navigate to the host.
2. Click the **Configure** tab.
3. Select **Networking**, and click **VMkernel adapters**.
4. Click **Add networking**.
5. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
6. On the Select target device page, select the switch for the VMkernel adapter, and click **Next**.

Option	Description
Select an existing network	Use the physical adapter configuration of an existing distributed port group to send data from the VMkernel adapter to the external network.
Select an existing standard switch	Use the physical adapter configuration for the VMkernel adapter of an existing

Option	Description
	standard switch.
New vSphere standard switch	Assign a new physical adapter configuration for the VMkernel adapter on a new standard switch.

7. On the Port properties page, select **Provisioning** from the **TCP/IP stack** drop-down menu.

   The provisioning traffic becomes the only service that is enabled. You cannot use this VMkernel adapter for traffic types other than provisioning.

8. Set the label, VLAN ID, and IP mode of the VMkernel adapter, and click **Next**.

9. Optional: On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter.

Option	Description
	The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack. Select the **Override default gateway for this adapter** check box and enter a gateway address, if you want to specify a different gateway for the VMkernel adapter. **Note:** Selected netstack should have the default gateway explicitly on

Option	Description
	each host.

10. Optional: On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisemer to obtain IPv6 addresses. In ESXi 6.5 and later router advertisemer is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	1. Click **Add IPv6**

Option	Description
	address to add a new IPv6 address. 2. Enter the IPv6 address and subnet prefix length, and click **OK**. 3. To change the VMkerne default gateway, click **Overrid default gateway for this adapter**. The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

11. Review your settings selections on the Ready to complete page and click **Finish**.

After you create a VMkernel adapter on the provisioning TCP/IP stack, you can use only this stack for cold migration, cloning, and snapshots on this host. The VMkernel adapters on the default TCP/IP stack are deactivated for the provisioning service. If a live migration uses the default TCP/IP stack while you configure VMkernel adapters with the provisioning TCP/IP stack, the data transfer completes successfully. However, the involved VMkernel adapters on the default TCP/IP stack are deactivated for future cold migration, cross-host cloning, and snapshot sessions.

Limits on Simultaneous Migrations

vCenter Server places limits on the number of simultaneous virtual machine migration and provisioning operations that can occur on each host, network, and datastore.

Each operation, such as a migration with vMotion or cloning a virtual machine, is assigned a resource cost. Each host, datastore, or network resource, has a maximum cost that it can support at any one time. Any new migration or provisioning operation that causes a resource to exceed its maximum cost does not proceed immediately, but is queued until other operations complete and release resources. Each of the network, datastore, and host limits must be satisfied for the operation to proceed.

vMotion without shared storage, migrating virtual machines to a different host and datastore simultaneously, is a combination of vMotion and Storage vMotion. This migration inherits the network, host, and datastore costs associated with those operations. vMotion without shared storage is equivalent to a Storage vMotion with a network cost of 1.

Network Limits

Network limits apply only to migrations with vMotion. Network limits depend on the version of ESXi and the network type. All migrations with vMotion have a network resource cost of 1.

Table 147: Network Limits for Migration with vMotion

Operation	ESXi Version	Network Type	Maximum Cost
vMotion	6.0, 6.5, 6.7, 7.0	1GigE	4
vMotion	6.0, 6.5, 6.7, 7.0	10GigE	8

Datastore Limits

Datastore limits apply to migrations with vMotion and with Storage vMotion. A migration with vMotion has a resource cost of 1 against the shared virtual machine's datastore. A migration with Storage vMotion has a resource cost of 16 against the source datastore and 16 against the destination datastore.

Table 148: Datastore Limits and Resource Costs for vMotion and Storage vMotion

Operation	ESXi Version	Maximum Cost Per Datastore	Datastore Resource Cost
vMotion	6.0, 6.5, 6.7, 7.0	128	1
Storage vMotion	6.0, 6.5, 6.7, 7.0	128	16

Host Limits

Host limits apply to migrations with vMotion, Storage vMotion, and other provisioning operations such as cloning, deployment, and cold migration. All hosts have a maximum cost per host of 8. For example, on an ESXi 7.0 host, you can perform 2 Storage vMotion operations, or 1 Storage vMotion and 4 vMotion operations.

Table 149: Host Migration Limits and Resource Costs for vMotion, Storage vMotion, and Provisioning Operations

Operation	ESXi Version	Derived Limit Per Host	Host Resource Cost
vMotion	6.0, 6.5, 6.7, 7.0	8	1
Storage vMotion	6.0, 6.5, 6.7, 7.0	2	4

Operation	ESXi Version	Derived Limit Per Host	Host Resource Cost
vMotion Without Shared Storage	6.0, 6.5, 6.7, 7.0	2	4
Other provisioning operations	6.0, 6.5, 6.7, 7.0	8	1

Migration Compatibility Checks

During migration, use the **Migrate Virtual Machine** wizard to view information about the compatibility checks carried out using various criteria between the destination host or cluster and the migrating virtual machine.

When you select a host or a cluster, the Compatibility panel at the bottom of the **Migrate Virtual Machine** wizard displays information about the compatibility of the selected host or cluster with the virtual machine's configuration.

Compatibility Check Results

If the virtual machine is compatible, the panel displays the message `Compatibility checks succeeded`. If the virtual machine is not compatible with either the host's or cluster's configured networks or datastores, the compatibility window might display both warnings and errors:

- Warning messages do not stop migration. Often the migration is justified and you can continue with the migration despite the warnings.
- Errors might stop migration if no error-free destination hosts are available among the selected destination hosts. In this case, if you click **Next**, the wizard displays the compatibility errors again, and you cannot proceed to the next step.

Compatibility Checks During Migration Setup

When you attempt to move only the compute resource, the **Migrate Virtual Machine** wizard examines the source and destination hosts, the target resource pool, the datastore, and the network. When you attempt to move only the storage, the wizard checks the compatibility of the same objects except for the network.

When you move compute resources and storage together, the **Migrate Virtual Machine** wizard runs fewer compatibility checks. For example, if you move the compute resource, you select the target host or cluster under a vCenter Server instance. The wizard performs all necessary validation only against the selected host, and does not check the datastores available on the destination host. When you attempt to move the virtual machine to a cluster, the **Migrate Virtual Machine** wizard examines the compatibility against the host recommendation from vSphere DRS. The wizard directly validates the compatibility of the target datastore when you select it later.

Another compatibility check is whether vMotion is enabled on the source and target hosts.

Compatibility Checks for Virtual Hardware

Effects of a specific host CPU feature on compatibility depend on whether ESXi exposes or hides them from virtual machines.

- Features that are exposed to virtual machines are not compatible when they do not match on the source and target hosts.
- Features that are not exposed to virtual machines are considered as compatible regardless of whether they match on the hosts.

Specific items of virtual machine hardware can also cause compatibility problems. For example, a virtual machine using an Enhanced VMXNET virtual NIC cannot be migrated to a host running a version of ESXi that does not support Enhanced VMXNET.

Working with the Developer Center

The Developer Center is a single point of entry for developers that provides tools to manage API structure and to capture user actions to translate them into executable code.

Using the API Explorer

The API Explorer allows you to browse and invoke vSphere REST APIs supported by the system and provides information and context around the API calls.

With the API Explorer, you can choose an API endpoint from your environment and retrieve a list of vSphere REST APIs. You can review details like available parameters, expected responses, and response status codes, and you can invoke the APIs against the live environment. The available APIs depend on the role of the selected endpoint.

Retrieve APIs Using API Explorer

API Explorer retrieves available vSphere REST APIs from a selected endpoint to give you information and context around API calls.

1. On the vSphere Client home page, click **Developer Center** and select the **API Explorer** tab.
2. From the **Select Endpoint** drop-down menu, select an endpoint from the environment.
3. From the **Select API** drop-down menu, select an API. The listed APIs are the ones publicly provided by the API explorer in vCenter Server.
4. Optional: You can use the filter text box to filter your results. For example, enter `health` to view a list of methods related to monitoring the health of the selected API.
5. Select an API category from the list.
6. Select a method from the list.

   You can review deprecated APIs by using the toggle button next to each method from the list. Avoid using deprecated APIs. Deprecated APIs might become unresponsive in the future and cause unexpected failures in your automation scripts.

   Detailed information about the method appears.
7. If a section about parameter details appears for the selected method, enter a method parameter value in the **Value** text box.
8. Optional: To invoke the method against the live environment, click **Execute**.
   a) If a warning dialog box appears, click **Yes**.

   The result for the invoked method appears in the response box.
9. Optional: To copy the result for the invoked method to your clipboard, click **Copy Response**.
10. Optional: To download the result for the invoked method, click **Download**.

Using Code Capture

Code Capture records user actions and translates them into executable code.

Record Actions Using Code Capture

To use Code Capture to record a session, you must first enable Code Capture.

Note: Calls made on operations regarding roles, privileges, tags, content libraries, and storage policies are not recorded. Sensitive data such as passwords is not recorded.

1. From the home sidebar menu, click **Developer Center** and go to the **Code Capture** tab.
2. Optional: If Code Capture is not enabled, click the toggle to enable Code Capture.
3. To start a recording, navigate to your desired pane and click the red record button in the top pane. To start recording immediately, click **Start Recording**.

   While a recording is in progress, the red record button in the top pane blinks.
4. Optional: To clear the code captured in a previous session and start a new session, click **Clear and Start Another**.
5. To stop a recording, click the red record button in the top pane, or navigate to the **Code Capture** tab in the Developer Center and click **Stop Recording**.

   The recorded code appears in the code pane.
6. Optional: Click **Copy** to copy the code or **Download** to download it as a PowerCLI script.
7. To clear the current code and start another recording, click **Clear and Start Another** or navigate to your desired pane and click the red record button in the top pane.

The recorded code appears in the code pane. You can copy the code, download it, or clear the code to start another recording.

Automating Management Tasks Using vRealize Orchestrator

VMware™vRealize Orchestrator is a platform that provides a library of extensible workflows. By using the workflow library, you can automate and configure processes to manage the vSphere infrastructure, other VMware technologies, and third-party technologies.

vRealize Orchestrator exposes every operation in the vCenter Server API so that you can integrate all these operations into your own automated processes.

Concepts of Workflows

A workflow is a series of actions and decisions that are automated to run sequentially after you run the workflow. vRealize Orchestrator provides a library of workflows that perform common management tasks.

Basics of Workflows

Workflows consist of a schema, variables, and input and output parameters. The workflow schema is the main component of a workflow as it defines all the workflow elements and the logical task flow of the workflow. The workflow variables and parameters are used by workflows to transfer data. vRealize Orchestrator saves a workflow token every time a workflow runs, recording the details of that specific run of the workflow. This token contains all parameters related to the workflow run. For example, if you run a workflow three times, three workflow tokens are saved.

With the vSphere Client, you can run and schedule workflows on selected objects from the vSphere inventory. You cannot create, delete, edit, and manage workflows in the vSphere Client. You develop and manage workflows in the vRealize Orchestrator client. For more information about the vRealize Orchestrator client, see *Using the VMware vRealize OrchestratorK Client*.

Input Workflow Parameters

To run, most workflows require a certain set of input parameters. The workflow processes input parameters that the user, an application, another workflow, or an action passes to it.

For example, if a workflow resets a virtual machine, the workflow requires the name of the virtual machine as an input parameter.

Output Workflow Parameters

The workflow output parameters represent the result from the workflow run. Some workflows and workflow elements can change the output parameters of the workflow when they run. While they run, workflows can receive the output parameters of other workflows as input parameters.

For example, if a workflow creates a snapshot of a virtual machine, the output parameter for the workflow is the resulting snapshot.

Workflow Presentation

When you run a workflow in the vSphere Client, the client loads the workflow presentation. You provide the input parameters of the workflow in the workflow presentation.

Waiting for Input

Some workflows require user input during their run and the run is suspended either until the user provides the required information, or until the workflow run times out.

Performing Administration Tasks on the vSphere Objects

By using the Orchestrator view in the vSphere Client, you can perform administration tasks such as running and scheduling workflows, and viewing the list of available workflows.

From the Orchestrator view in the vSphere Client, you can perform the following tasks:

- Select a default vRealize Orchestrator server.
- Work with workflows. Working with workflows includes the following tasks:
  - Associating workflows with specific vSphere inventory objects such as virtual machines, ESXi hosts, clusters, resource pools, and folders.
  - Exporting and importing existing associations of workflows with vSphere inventory objects for backup purposes or to import them to another vCenter Server instance.
  - Editing associations of workflows with vSphere inventory objects such as virtual machines, ESXi hosts, clusters, resource pools, folders, and others.
  - Viewing information about workflow runs and about workflows waiting for user intervention.
  - Running and scheduling workflows on vSphere objects.

To run workflows on specific vSphere inventory objects, you must select a default vRealize Orchestrator server. Associate the workflows of the default vRealize Orchestrator server with the vSphere inventory objects that you want to manage.

Configure the Default vRealize Orchestrator

You configure multiple Orchestrator servers to work with a vCenter Server instance that is connected to your vSphere Client. A default Orchestrator server is automatically configured to work with the vCenter Server instance, unless you configure one manually. Otherwise, a default Orchestrator server is automatically selected.

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You

register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

1. Log in to the vSphere Client as a member of the Administrators group.
2. In the object navigator, click **vRealize Operations**.
3. In the **Manage** tab, click the **Servers** subtab.

   A table appears that lists the available vCenter Server instances. Each row of the table contains a vCenter Server and the Orchestrator server that manages it.
4. Click **Edit configuration**.
5. In the **Edit vRealize Orchestrator connections** dialog box, select the default Orchestrator server to manage your vCenter Server instance.
   - Select the **Fixed IP/host name** option and enter the IP address of the Orchestrator server.
   - Select the **Registered as VC extension** option and from the drop-down menu, select the URL address of the Orchestrator server.
6. Click **OK**.

You successfully configured a default vRealize Orchestrator server in the vSphere Client.

Managing Associations of Workflows with vSphere Inventory Objects

You can associate workflows with the different vSphere object types to see more workflows displayed in the context menu when you right-click a vSphere inventory object. You can also run these workflows on more object types.

You can add and edit associations, and export and import XML files containing the associations of workflows with vSphere objects.

Workflows associated with inventory object types are listed in the context menu that appears when you right-click the inventory objects and in the **Actions** menu.

Only users from the Orchestrator Administrator group have the rights to manage the associations of workflows with vSphere inventory objects.

Associate Workflows with vSphere Inventory Object Types

You can associate workflows with a vSphere object type, such as host, to run the workflows directly on the inventory objects of that type.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

- Log in to the vSphere Client as a member of the Administrators group.

Workflows associated with inventory object types are listed in the context menu that appears when you right-click an inventory object, and in the **Actions** menu.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click the **Manage** tab.
3. Click the **Context Actions** subtab.
4. Click the **Add** icon to add a workflow.
5. Select the Orchestrator server from the vRO Servers tree, and navigate through the workflow library to find the workflow to add.
6. Click **Add**.
   The workflow appears in the list of selected workflows on the right.
7. Optional: Enable multi-selection.
   With multi-selection enabled, you can select multiple vSphere objects of the same type when you run the workflow.
8. Under Available types, select the vSphere object types with which you want to associate the workflow.
9. Click **OK**.

Edit the Associations of Workflows with vSphere Objects

You can associate a workflow with different objects from the vSphere inventory and also edit the associations of workflows with the objects from the vSphere inventory.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which the vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*
- Log in as a member of the Administrators group to configure the default Orchestrator server.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click the **Manage** tab.
3. Click the **Context Actions** subtab.
4. Right-click the workflow to edit and select **Edit**.
5. Change the association properties.
6. Click **OK**.

Export the Associations of Workflows with vSphere Objects

You can transfer the associations of workflows with objects in the vSphere inventory using an XML file.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which the vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*

- Log in as a member of the Administrators group to configure the default Orchestrator server.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click the **Manage** tab.
3. Click the **Context Actions** subtab.
4. Click the **Export** icon .
5. Select a location where you want to save the XML file, and click **Save**.

Import the Association of Workflows with vSphere Objects

You can import an XML file that contains the association of workflows with objects in the vSphere inventory.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*
- Log in as a member of the Administrators group to configure the default Orchestrator server.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click the **Manage** tab.
3. Click the **Context Actions** subtab.
4. Click the **Import** icon .
5. Browse to select the XML file to import and click **Open**.

Orchestrator compares the two associated workflow sets and imports the missing workflow associations.

Working with Workflows

You can view information about Orchestrator workflows, run, and schedule workflows by using the vSphere Client.

You can perform some scheduling and running tasks on the Orchestrator workflows from the vRealize Orchestrator view in the vSphere Client. You can schedule a workflow to run at a specified time or start a workflow directly, by right-clicking a vSphere inventory object and selecting **All vRealize Orchestrator plugin Actions**.

Workflow tasks include:

- Running workflows on vSphere inventory objects, such as virtual machines, ESXi hosts, clusters, resource pools, and folders.
- Viewing information about workflow runs.
- Viewing information about workflows waiting for user interaction.
- Searching for a specific workflow from the list of available workflows.
- Scheduling workflows.

Run Workflows on vSphere Inventory Objects

You can automate management tasks in vSphere by running Orchestrator workflows directly on objects from the vSphere inventory.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which the vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter

Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*

- Verify that you have workflows associated with the vSphere inventory objects. See Associate Workflows with vSphere Inventory Object Types.

1. Click **vCenter**.
2. Under Inventory Lists, click an inventory category.
3. Right-click the object that you want to run the workflow on, and navigate to **All vRealize Orchestrator plugin Actions**.

   All available workflows that you can run on the selected inventory object are listed.
4. Click the workflow that you want to run.

   Note: If you cannot find the expected workflows, you might need to associate them to the specified vSphere inventory object.
5. Click the **Start/Schedule** menu option.
6. Optional: Select Run now to start the workflow run immediately.
7. Provide the required workflow parameters.
8. Optional: Select Schedule to configure the workflow to run at a specified time.
   a) In the **Task name** text box, type the name of the scheduled task.
   b) Optional: In the **Description** text box, type a description of the scheduled task.
   c) Schedule the date and time of the workflow run.
   d) Specify the recurrence options.
9. Click **Finish**.

View Information About Workflow Runs

You can view information about the workflow runs for each connected Orchestrator server. The available information includes the workflow name, start and end date, state of the workflow, and the user who started the workflow.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.
- Run an Orchestrator workflow.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click **vRO Servers**.

   A list of the available vRealize Orchestrator servers appears.
3. Click a vRealize Orchestrator server, and click the **Monitor** tab.

   The list of workflow runs appears.

You can review the list of workflow runs, cancel a running workflow, or respond to a workflow that requires interaction.

View Information About the Runs of a Specific Workflow

You can view information about the runs of a single workflow such as start and end date, state of the workflow, and user who has started the workflow.

- Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Serverextension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.
- Run the specific Orchestrator workflow at least once.

1. In the object navigator, click **vRealize Orchestrator**.
2. Under Inventory Lists, click **Workflows**.
   A list of the available workflows appears.
3. Click the name of a workflow, and click the **Monitor** tab.
   A list of workflow runs appears.

You can review the list of workflow runs, cancel a running workflow, or respond to a workflow that requires interaction.

View Workflows That Are Waiting for User Interaction

You can view the workflows that are waiting for a user interaction.

1. Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*
2. In the object navigator, click **vRealize Orchestrator**.
3. Under Inventory lists, click **Waiting for interaction**.

A list of workflows that are waiting for a user interaction appears.
You can provide values for the required parameters of workflows that are waiting for a user interaction.

Searching for Workflows

You can browse for workflows in the inventory of the Orchestrator server or filter the available workflows by a search keyword to find a particular workflow.

Browse the Inventory of the Orchestrator Server

You can view the available workflows in the inventory of each connected Orchestrator server. You can search for a particular type of workflow by browsing the workflow categories.

1. Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*
2. In the object navigator, click **vRealize Orchestrator**.
3. Click **vRO Servers**.
   A list of the available vRealize Orchestrator servers appears

4. Double-click a vRealize Orchestrator server.
5. Click **Categories**.
6. Double-click **Library**.

   Note: **Library** is the default main workflow category. An Orchestrator server can have additional custom workflow categories.
7. Click **Categories**.

   A list of available workflow categories appears.
8. Double-click a workflow category to browse the available workflows and its subcategories.

Find a Workflow

If you have many workflows, you can filter them by a search keyword to find a specific workflow.

1. Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.
2. In the object navigator, click **vRealize Orchestrator**.
3. Click **Workflows**.
4. In the **Filter** text box, type a search term or the name of the workflow that you are searching for.

   A list displays the workflows that contain the search term in the workflow name or description.

Scheduling Workflows

You can create tasks to schedule workflows, edit scheduled tasks, suspend scheduled tasks, and resume suspended scheduled tasks.

Schedule a Workflow

You can schedule a workflow to run at a specified time. You can also set the recurrence for a scheduled workflow.

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You

register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

1. In the object navigator, click **vRealize Orchestrator**.
2. Under Inventory Lists click **Workflows**.
3. Right-click the workflow that you want to schedule and select **Schedule a workflow**.
4. Provide the required workflow parameters.
5. Click **Start/Schedule**.
6. In the **Task name** text box, type the name of the scheduled task.
7. Optional: In the **Description** text box, type a description of the scheduled task.
8. Schedule the date and time of the workflow run.
9. Specify the recurrence options.
10. Click **Finish**.

Edit the Schedule of a Workflow

You can modify the schedule of a workflow and set it to run at an earlier or later time.

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click **Scheduled workflows**.
   A list of the scheduled workflows appears.
3. Right-click the workflow whose schedule you want to edit and select **Edit**.
4. In the **Task name** text box, type the new name of the scheduled task.
5. Optional: In the **Description** text box, type a description of the scheduled task.
6. Edit the scheduled date and time of the workflow run.
7. Specify the recurrence options.
8. Click **Finish**.

Run a Scheduled Workflow

You can manually run a scheduled workflow before it runs automatically.

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

When you run a workflow manually, the schedule is not affected. After the manual run, the workflow runs again at the scheduled time.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click **Scheduled workflows**.
   A list of the scheduled workflows appears.

3. Click **Scheduled workflows**.
4. Right-click the workflow that you want to run and select **Run now**.

You can view information about the workflow run in the Recent Tasks pane or in the Orchestrator server menu. See View Information About Workflow Runs.

Suspend a Scheduled Task

You can suspend a scheduled workflow run. You can also resume suspended scheduled tasks.

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click **Scheduled workflows**.
   A list of the scheduled workflows appears.
3. Right-click a workflow and select **Suspend**.
   The workflow schedule is suspended.

The state of the scheduled task changes to Suspended.

Resume a Suspended Scheduled Task

You can resume a scheduled task that has been suspended.

Verify that you have configured at least one Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Serverextensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

1. In the object navigator, click **vRealize Orchestrator**.
2. Click **Scheduled workflows**.
   A list of the scheduled workflows appears.
3. Right-click a workflow and select **Resume**.
   The workflow schedule is resumed from suspension.

The state of the scheduled task changes to Pending.

Workflows for Managing Inventory Objects

The default workflows for managing vSphere inventory objects are the workflows included in the vCenter Server plug-in workflow library. The vCenter Server plug-in workflow library contains workflows that you can use to run automated processes related to the vCenter Server and host management.

To access workflows in the vSphere Client, make sure that you configure at least one running Orchestrator server to work with the same Single Sign-On instance to which vCenter Server is pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user account that has the necessary privileges to manage vCenter Server extensions. For more information, see *Installing and Configuring VMware vRealize OrchestratorK*.

Note: Only a predefined set of vCenter Server workflows are available by default in the context menu. You can associate additional workflows with each vSphere object. See Associate Workflows with vSphere Inventory Object Types.

Cluster and Compute Resource Workflows

With the cluster and compute resource workflows, you can create, rename, or delete a cluster. You can also activate or deactivate high availability, Distributed Resource Scheduler, and vCloud Distributed Storage on a cluster.

Workflow Name	Description
Add DRS virtual machine group to cluster	Adds a DRS virtual machine group to a cluster.
Add virtual machines to DRS group	Adds a virtual machine list to an existing DRS virtual machine group.
Create cluster	Creates a cluster in a host folder.
Delete cluster	Deletes a cluster.
Disable DRS on cluster	Deactivates DRS on a cluster.
Disable HA on cluster	Deactivates high availability on a cluster.
Disable vCloud Distributed Storage on cluster	Deactivates vCloud Distributed Storage on a cluster.
Enable DRS on cluster	Enables DRS on a cluster.
Enable HA on cluster	Enables high availability on a cluster.
Enable vCloud Distributed Storage on cluster	Enables vCloud Distributed Storage on a cluster.
Remove virtual machine DRS group from cluster	Removes a DRS virtual machine group from a cluster.
Remove virtual machines from DRS group	Removes virtual machines from a cluster DRS group.
Rename cluster	Renames a cluster.

Guest Operation Files Workflows

With the guest operation files workflows, you can manage files in a guest operating system.

Check for directory in guest	Verifies that a directory exists in a guest virtual machine.
Check for file in guest	Verifies that a file exists in a guest virtual machine.
Copy file from guest to Orchestrator	Copies a specified file from a guest file system to an Orchestrator server.
Copy file from Orchestrator to guest	Copies a specified file from an Orchestrator server to a guest file system.
Create directory in guest	Creates a directory in a guest virtual machine.
Create temporary directory in guest	Creates a temporary directory in a guest virtual machine.
Create temporary file in guest	Creates a temporary file in a guest virtual machine.
Delete directory in guest	Deletes a directory from a guest virtual machine.
Delete file in guest	Deletes a file from a guest virtual machine.
List path in guest	Shows a path in a guest virtual machine.
Move directory in guest	Moves a directory in a guest virtual machine.
Move file in guest	Moves a file in a guest virtual machine.

Guest Operation Processes Workflows

With the guest operation processes workflows, you can get information and control the running processes in a guest operating system.

Get environment variables from guest	Returns a list with environmental variables from a guest. An interactive session returns the variables of the user who is logged in.

Get processes from guest	Returns a list with the processes running in the guest operating system and the recently completed processes started by the API.
Run program in guest	Starts an application in a guest operating system.
Kill process in guest	Terminates a process in a guest operating system.

Custom Attributes Workflows

With the custom attributes workflows, you can add custom attributes to virtual machines or get a custom attribute for a virtual machine.

Add custom attribute to a virtual machine	Adds a custom attribute to a virtual machine.
Add custom attribute to multiple virtual machines	Adds a custom attribute to a selection of virtual machines.
Get custom attribute	Gets a custom attribute for a virtual machine in vCenter Server.

Data Center Workflows

With the data center workflows, you can create, delete, reload, rename, or rescan a data center.

Create datacenter	Creates a data center in a data center folder.
Delete datacenter	Deletes a data center.
Reload datacenter	Forces vCenter Server to reload data from a data center.
Rename datacenter	Renames a data center and waits for the task to complete.
Rescan datacenter HBAs	Scans the hosts in a data center and initiates a rescan on the host bus adapters to discover new storage.

Datastore and Files Workflows

With the datastore and files workflows, you can delete a list of files, find unused files in a datastore, and others.

Delete all files	Deletes a list of files.
Delete all unused datastore files	Searches all datastores in the vCenter Server environment and deletes all unused files.
Export unused datastore files	Searches all datastores and creates an XML descriptor file that lists all unused files.
Find unused files in datastores	Searches the vCenter Server environment for all unused disks (`*.vmdk`), virtual machines (`*.vmx`), and template (`*.vmtx`) files that are not associated with any vCenter Server instances registered with Orchestrator.
Get all configuration, template, and disk files from virtual machines	Creates a list of all virtual machine descriptor files and a list of all virtual machine disk files, for all datastores.
Log all datastore files	Creates a log for every virtual machine configuration file and every virtual machine file found in all datastores.
Log unused datastore files	Searches the vCenter Server environment for unused files that are registered on virtual machines and exports a log of the files in a text file.
Upload file to datastore	Uploads a file to an existing folder on a specific datastore. The uploaded file overwrites any existing file with the same name in the same destination folder.

Data Center Folder Management Workflows

With the data center folder management workflows, you can create, delete, or rename a data center folder.

Create datacenter folder	Creates a data center folder.
Delete datacenter folder	Deletes a data center folder and waits for the task to complete.
Rename datacenter folder	Renames a data center folder and waits for the task to complete.

Host Folder Management Workflows

With the host folder management workflows, you can create, delete, or rename a host folder.

Create host folder	Creates a host folder.
Delete host folder	Deletes a host folder and waits for the task to complete.
Rename host folder	Renames a host folder and waits for the task to complete.

Virtual Machine Folder Management Workflows

With the virtual machine folder management workflows, you can create, delete, or rename a virtual machine folder.

Create virtual machine folder	Creates a virtual machine folder.
Delete virtual machine folder	Deletes a virtual machine folder and waits for the task to complete.
Rename virtual machine folder	Renames a virtual machine folder and waits for the task to complete.

Basic Host Management Workflows

With the basic host management workflows, you can put a host into maintenance mode, make a host exit maintenance mode. You can also move a host to a folder or a cluster, and reload data from a host.

Enter maintenance mode	Puts the host into maintenance mode. You can cancel the task.
Exit maintenance mode	Exits maintenance mode. You can cancel the task.
Move host to cluster	Moves an existing host into a cluster. The host must be part of the same data center, and if the host is part of a cluster, the host must be in maintenance mode.
Move host to folder	Moves a host into a folder as a standalone host. The host must be part of a ClusterComputeResource in the same data center and the host must be in maintenance mode.
Reload host	Forces vCenter Server to reload data from a host.

Host Power Management Workflows

With the host power management workflows, you can reboot or shut down a host.

Reboot host	Reboots a host. If the Orchestrator client is connected directly to the host, it loses the connection to the host and does not receive an indication of success in the returned task.
Shut down host	Shuts down a host. If the Orchestrator client is connected directly to the host, it loses the connection to the host and does not receive an indication of success in the returned task.

Host Registration Management Workflows

With the host registration management workflows, you can add a host to a cluster, disconnect or reconnect a host from a cluster, and others.

Add host to cluster	Adds a host to the cluster. This workflow fails if it cannot authenticate the SSL certificate of the host.
Add standalone host	Registers a host as a standalone host.
Disconnect host	Disconnects a host from vCenter Server.
Reconnect host	Reconnects a disconnected host by providing only the host information.
Reconnect host with all information	Reconnects a disconnected host by providing all information about the host.
Remove host	Removes a host and unregisters it from vCenter Server. If the host is part of a cluster, you must put it in maintenance mode before attempting to remove it.

Networking Workflows

With the networking workflows, you can add a port group to distributed virtual switch, create a distributed virtual switch with a port group, and others.

Add port group to distributed virtual switch	Adds a new distributed virtual port group to a specified distributed virtual switch.
Attach host system to distributed virtual switch	Adds a host to a distributed virtual switch.
Create distributed virtual switch with port group	Creates a distributed virtual switch with a distributed virtual port group.

Distributed Virtual Port Group Workflows

With the distributed virtual port group workflows, you can update or delete a port group, and reconfigure the port group.

Connect virtual machine NIC number to distributed virtual port group	Reconfigures the network connection of the specified virtual machine NIC number to connect to the specified distributed virtual port group. If no NIC number is specified, the number zero is used.
Delete distributed virtual port group	Deletes a specified distributed virtual port group.
Set teaming options	Provides an interface to manage the teaming options for a distributed virtual port group.
Update distributed virtual port group	Updates the configuration of a specified distributed virtual port group.

Distributed Virtual Switch Workflows

With the distributed virtual switch workflows, you can create, update, or delete a distributed virtual switch, and create, delete, or update a private VLAN.

Create distributed virtual switch	Creates a distributed virtual switch in the specified network folder with a name and uplink port names that you specify. You must specify at least one uplink port name.
Create private VLAN	Creates a VLAN on the specified distributed virtual switch.
Delete distributed virtual switch	Deletes a distributed virtual switch and all associated elements.
Delete private VLAN	Deletes a VLAN from a specified distributed virtual switch. If a secondary VLAN exists, you must first delete the secondary VLAN.
Update distributed virtual switch	Updates the properties of a distributed virtual switch.
Update private VLAN	Updates a VLAN on the specified distributed virtual switch.

Standard Virtual Switch Workflows

With the standard virtual switch workflows, you can create, update, or delete a standard virtual switch, and create, delete, or update port groups in standard virtual switches.

Add port group in standard virtual switch	Adds a port group in a standard virtual switch.
Create standard virtual switch	Creates a standard virtual switch.
Delete port group from standard virtual switch	Deletes a port group from a standard virtual switch.
Delete standard virtual switch	Deletes a standard virtual switch from a host's network configuration.
Retrieve all standard virtual switches	Retrieves all standard virtual switches from a host.
Update port group in standard virtual switch	Updates the properties of a port group in a standard virtual switch.
Update standard virtual switch	Updates the properties of a standard virtual switch.
Update vNIC for port group in standard virtual switch	Updates a vNIC associated with a port group in a standard virtual switch.

Resource Pool Workflows

With the resource pool workflows, you can create, rename, reconfigure or delete a resource pool, and get resource pool information.

Create resource pool	Creates a resource pool with the default CPU and memory allocation values. To create a resource pool in a cluster, the cluster must have VMware DRS enabled.
Create resource pool with specified values	Creates a resource pool with CPU and memory allocation values that you specify. To create a resource pool in a cluster, the cluster must have VMware DRS enabled.
Delete resource pool	Deletes a resource pool and waits for the task to complete.
Get resource pool information	Returns CPU and memory information about a given resource pool.
Reconfigure resource pool	Reconfigures CPU and memory allocation configuration for a given resource pool.
Rename resource pool	Renames a resource pool and waits for the task to complete.

Storage Workflows

With the storage workflows, you can perform storage-related operations.

Workflow Name	Description
Add datastore on iSCSI/FC/local SCSI	Creates a datastore on a Fibre Channel, iSCSI or local SCSI disk. Only disks that are not currently in use by an existing VMFS are applicable to new datastore creation. The new datastore allocates the maximum available space of the specified disk.
Add datastore on NFS	Adds a datastore on an NFS server.
Add iSCSI target	Adds iSCSI targets to a vCenter Server host. The targets can be of the type `Send` or `Static`.
Create VMFS for all available disks	Creates a VMFS volume for all available disks of a specified host.
Delete datastore	Deletes datastores from a vCenter Server host.
Delete iSCSI target	Deletes already configured iSCSI targets. The targets can be of type `Send` or `Static`.

Workflow Name	Description
Disable iSCSI adapter	Deactivates the software iSCSI adapter of a specified host.
Display all datastores and disks	Displays the existing datastores and available disks on a specified host.
Enable iSCSI adapter	Enables an iSCSI adapter.
List all storage adapters	Lists all storage adapters of a specified host.

Storage DRS Workflows

With the storage DRS workflows, you perform storage-related operations. These include creating and configuring a datastore cluster, removing a datastore from a cluster, adding storage to a cluster, and others.

Add datastore to cluster	Adds datastores to a datastore cluster. Datastores must be able to connect to all hosts to be included in the datastore cluster. Datastores must have the same connection type to reside within a datastore cluster.
Change Storage DRS per virtual machine configuration	Sets Storage DRS settings for each virtual machine.
Configure datastore cluster	Configures datastore cluster setting values for automation and runtime rules.
Create simple datastore cluster	Creates a simple datastore cluster with default configuration. The new datastore cluster contains no datastores.
Create Storage DRS scheduled task	Creates a scheduled task for reconfiguring a datastore cluster. Only automation and runtime rules can be set.
Create virtual machine anti-affinity rule	Creates an anti-affinity rule to indicate that all virtual disks of certain virtual machines must be kept on different datastores.
Create VMDK anti-affinity rule	Creates a VMDK anti-affinity rule for a virtual machine that indicates which of its virtual disks must be kept on different datastores. The rule applies to the virtual disks of the selected virtual machine.
Remove datastore cluster	Removes a datastore cluster. Removing a datastore cluster also removes all the settings and the alarms for the cluster from the vCenter Server system.
Remove datastore from cluster	Removes a datastore from a datastore cluster and puts the datastore in a datastore folder.
Remove Storage DRS scheduled task	Removes a scheduled Storage DRS task.
Remove virtual machine anti-affinity rule	Removes a virtual machine anti-affinity rule for a given datastore cluster.
Remove VMDK anti-affinity rule	Removes a VMDK anti-affinity rule for a given datastore cluster.

Basic Virtual Machine Management Workflows

With the basic virtual machine management workflows, you can perform basic operations on virtual machines, for example, create, rename, or delete a virtual machine, upgrade virtual hardware, and others.

Create custom virtual machine	Creates a virtual machine with the specified configuration options and additional devices.
Create simple dvPortGroup virtual machine	Creates a simple virtual machine. The network used is a Distributed Virtual Port Group.
Create simple virtual machine	Creates a virtual machine with the most common devices and configuration options.

Delete virtual machine	Removes a virtual machine from the inventory and datastore.
Get virtual machines by name	Returns a list of virtual machines from all registered vCenter Server instances that match the provided expression.
Mark as template	Converts an existing virtual machine to a template, not allowing it to start. You can use templates to create virtual machines.
Mark as virtual machine	Converts an existing template to a virtual machine, allowing it to start.
Move virtual machine to folder	Moves a virtual machine to a specified virtual machine folder.
Move virtual machine to resource pool	Moves a virtual machine to a resource pool. If the target resource pool is not in the same cluster, you must use the migrate or relocate workflows.
Move virtual machines to folder	Moves several virtual machines to a specified virtual machine folder.
Move virtual machines to resource pool	Moves several virtual machines to a resource pool.
Register virtual machine	Registers a virtual machine. The virtual machine files must be placed in an existing datastore and must not be already registered.
Reload virtual machine	Forces vCenter Server to reload a virtual machine.
Rename virtual machine	Renames an existing virtual machine on the vCenter Server system or host and not on the datastore.
Set virtual machine performance	Changes performance settings such as shares, minimum and maximum values, shaping for network, and disk access of a virtual machine.
Unregister virtual machine	Removes an existing virtual machine from the inventory.
Upgrade virtual machine hardware (force if required)	Upgrades the virtual machine hardware to the latest revision that the host supports. This workflow forces the upgrade to continue, even if VMware Tools is out of date. If the VMware Tools is out of date, forcing the upgrade to continue reverts the guest network settings to the default settings. To avoid this situation, upgrade VMware Tools before running the workflow.
Upgrade virtual machine	Upgrades the virtual hardware to the latest revision that the host supports. An input parameter allows a forced upgrade even if VMware Tools is out of date.
Wait for task and answer virtual machine question	Waits for a vCenter Server task to complete or for the virtual machine to ask a question. If the virtual machine requires an answer, accepts user input and answers the question.

Clone Workflows

With the clone workflows, you can clone virtual machines with or without customizing the virtual machine properties.

Clone virtual machine from properties	Clones virtual machines by using properties as input parameters.
Clone virtual machine, no customization	Clones a virtual machine without changing anything except the virtual machine UUID.
Customize virtual machine from properties	Customizes a virtual machine by using properties as input parameters.

Linked Clone Workflows

With the linked clone workflows, you can perform linked clone operations, such as restoring a virtual machine from a linked clone, creating a linked clone, and others.

Restore virtual machine from linked clone	Removes a virtual machine from a linked clone setup.

Set up virtual machine for linked clone	Prepares a virtual machine to be link cloned.
Create a linked clone of a Linux machine with multiple NICs	Creates a linked clone of a Linux virtual machine, performs the guest operating system customization, and configures up to four virtual network cards.
Create a linked clone of a Linux machine with a single NIC	Creates a linked clone of a Linux virtual machine, performs the guest operating system customization, and configures one virtual network card.
Create a linked clone of a Windows machine with multiple NICs and credential	Creates a linked clone of a Windows virtual machine and performs the guest operating system customization. Configures up to four virtual network cards and a local administrator user account.
Create a linked clone of a Windows machine with a single NIC and credential	Creates a linked clone of a Windows virtual machine and performs the guest operating system customization. Configures one virtual network card and a local administrator user account.
Create a linked clone with no customization	Creates the specified number of linked clones of a virtual machine.

Linux Customization Clone Workflows

With the Linux customization workflows, you can clone a Linux virtual machine and customize the guest operating system.

Clone a Linux machine with multiple NICs	Clones a Linux virtual machine, performs the guest operating system customization, and configures up to four virtual network cards.
Clone a Linux machine with a single NIC	Clones a Linux virtual machine, performs the guest operating system customization, and configures one virtual network card.

Tools Clone Workflows

Use the tools clone workflows to obtain information about customizing the operating system of a virtual machine, updating a virtual device, and so on.

Get a virtual Ethernet card to change the network	Returns a new Ethernet card to update a virtual device. Contains only the device key of the given virtual device and the new network.
Get Linux customization	Returns the Linux customization preparation.
Get multiple virtual Ethernet card device changes	Returns an array of VirtualDeviceConfigSpec objects for add and remove operations on VirtualEthernetCard objects.
Get NIC setting map	Returns the setting map for a virtual network card by using VimAdapterMapping.
Get Windows customization for Sysprep with credentials	Returns customization information about the Microsoft Sysprep process, with credentials. Workflows for cloning Windows virtual machines use this workflow.
Get Windows customization for Sysprep with Unattended.txt	Returns customization information about the Microsoft Sysprep process by using an Unattended.txt file. Workflows for cloning Windows virtual machines use this workflow.
Get Windows customization for Sysprep	Returns customization information about the Microsoft Sysprep process. Workflows for cloning Windows virtual machines use this workflow.

Windows Customization Clone Workflows

With the Windows customization clone workflows, you can clone Windows virtual machines and customize the guest operating system.

Customize a Windows machine with single NIC and credential	Performs guest operating system customization, configures one virtual network card and a local administrator user account on a Windows virtual machine.
Clone a thin provisioned Windows machine with single NIC and credential	Clones a Windows virtual machine performing the guest operating system customization. Specifies virtual disk thin provisioning policy and configures one virtual network card and a local administrator user account. Sysprep tools must be available on the vCenter Server system.
Clone a Windows machine Sysprep with single NIC and credential	Clones a Windows virtual machine performing the guest operating system customization. Configures one virtual network card and a local administrator user account. Sysprep tools must be available on vCenter Server.
Clone a Windows machine with multiple NICs and credential	Clones a Windows virtual machine performing the guest operating system customization. Configures the local administrator user account and up to four virtual network cards. Sysprep tools must be available on the vCenter Server system.
Clone a Windows machine with single NIC	Clones a Windows virtual machine performing the guest operating system customization and configures one virtual network card. Sysprep tools must be available on the vCenter Server system.
Clone a Windows machine with single NIC and credential	Clones a Windows virtual machine performing the guest operating system customization. Configures one virtual network card and a local administrator user account. Sysprep tools must be available on the vCenter Server system.

Device Management Workflows

With the device management workflows, you can manage the devices that are connected to a virtual machine or to a datastore of a host.

Add CD-ROM	Adds a virtual CD-ROM to a virtual machine. If the virtual machine has no IDE controller, the workflow creates one.
Add disk	Adds a virtual disk to a virtual machine.
Change RAM	Changes the amount of RAM of a virtual machine.
Convert disks to thin provisioning	Converts thick-provisioned disks of virtual machines to thin-provisioned disks.
Convert independent disks	Converts all independent virtual machine disks to normal disks by removing the independent flag from the disks.
Disconnect all detachable devices from a running virtual machine	Disconnects floppy disks, CD-ROM drives, parallel ports, and serial ports from a running virtual machine.
Mount CD-ROM	Mounts the CD-ROM of a virtual machine. If the virtual machine has no IDE controller or CD-ROM drive, the workflow creates them.
Mount floppy disk drive	Mounts a floppy disk drive FLP file from the ESX datastore.

Move and Migrate Workflows

With the move and migrate workflows, you can migrate virtual machines.

Mass migrate virtual machines with Storage vMotion	Uses Storage vMotion to migrate a single virtual machine, a selection of virtual machines, or all available virtual machines.

Mass migrate virtual machines with vMotion	Uses vMotion, Storage vMotion, or both vMotion and Storage vMotion to migrate a single virtual machine, a selection of virtual machines, or all available virtual machines.
Migrate virtual machine with vMotion	Migrates a virtual machine from one host to another by using the `MigrateVM_Task` operation from the vSphere API.
Move virtual machine to another vCenter Server system	Moves a list of virtual machines to another vCenter Server system.
Quick migrate multiple virtual machines	Suspends the virtual machines if they are powered on and migrates them to another host using the same storage.
Quick migrate virtual machine	Suspends the virtual machine if it is powered on and migrates it to another host using the same storage.
Relocate virtual machine disks	Relocates virtual machine disks to another host or datastore while the virtual machine is powered off by using the `RelocateVM_Task` operation from the vSphere API.

Other Workflows

With the workflows in the Others category, you can activate and deactivate Fault Tolerance (FT), extract virtual machine information, and find orphaned virtual machines.

Workflow Name	Description
Disable FT	Deactivates Fault Tolerance for a specified virtual machine.
Enable FT	Enables Fault Tolerance for a specified virtual machine.
Extract virtual machine information	Returns the virtual machine folder, host system, resource pool, compute resource, datastore, hard drive sizes, CPU and memory, network, and IP address for a given virtual machine. Might require VMware Tools.
Find orphaned virtual machines	Lists all virtual machines in an orphaned state in the Orchestrator inventory. Lists the VMDK and VMTX files for all datastores in the Orchestrator inventory that have no association with any virtual machines in the Orchestrator inventory. Sends the lists by email (optional).
Get VM by Name and BIOS UUID	Searches virtual machines by name and then filters the result with particular universally unique identifier (UUID) in order to identify a unique virtual machine. **Note:** This workflow is needed when DynamicOps calls vRealize Orchestratorworkflows having input parameters of `VC:VirtualMachine` type in order to make the correspondence between a particular DynamicOps and vRealize Orchestrator virtual machine.
Get VM by Name and UUID	Searches virtual machines by name and then filters the result with particular universally unique identifier (UUID) in order to identify a unique virtual machine. **Note:** This workflow is needed when DynamicOps calls vRealize Orchestrator workflows having input parameters of `VC:VirtualMachine` type in order to make the correspondence between a particular DynamicOps and vRealize Orchestrator virtual machine.
Get VM UUID	Searches virtual machines by name and then filters the result with particular universally unique identifier (UUID) in order to identify a unique virtual machine.

Workflow Name	Description
	Note: This workflow is needed when DynamicOps calls vRealize Orchestrator workflows having input parameters of `VC:VirtualMachine` type in order to make the correspondence between a particular DynamicOps and vRealize Orchestrator virtual machine.

Power Management Workflows

With the power management workflows, you can power on and off virtual machines, reboot the guest operating system of a virtual machine, suspend a virtual machine, and others.

Power off virtual machine and wait	Powers off a virtual machine and waits for the process to complete.
Reboot guest OS	Reboots the virtual machine's guest operating system. Does not reset nonpersistent virtual machines. VMware Tools must be running.
Reset virtual machine and wait	Resets a virtual machine and waits for the process to complete.
Resume virtual machine and wait	Resumes a suspended virtual machine and waits for the process to complete.
Set guest OS to standby mode	Sets the guest operating system to standby mode. VMware Tools must be running.
Shut down and delete virtual machine	Shuts down a virtual machine and deletes it from the inventory and disk.
Shut down guest OS and wait	Shuts down a guest operating system and waits for the process to complete.
Start virtual machine and wait	Starts a virtual machine and waits for VMware Tools to start.
Suspend virtual machine and wait	Suspends a virtual machine and waits for the process to complete.

Snapshot Workflows

With the snapshot workflows, you can perform snapshot-related operations.

Create a snapshot	Creates a snapshot.
Create snapshots of all virtual machines in a resource pool	Creates a snapshot of each virtual machine in a resource pool.
Remove all snapshots	Removes all existing snapshots without reverting to a previous snapshot.
Remove excess snapshots	Finds virtual machines with more than a given number of snapshots and optionally deletes the oldest snapshots. Sends the results by email.
Remove old snapshots	Gets all snapshots that are older than a given number of days and prompts the user to select which ones to delete.
Remove snapshots of a given size	Gets all snapshots that are larger than a given size and prompts the user to confirm deletion.
Revert to current snapshot	Reverts to the current snapshot.
Revert to snapshot and wait	Reverts to a specific snapshot. Does not delete the snapshot.

VMware Tools Workflows

With the VMware Tools workflows, you can perform VMware Tools-related tasks on virtual machines.

Mount VMware tools installer	Mounts the VMware Tools installer on the virtual CD-ROM.
Set console screen resolution	Sets the console window's resolution. The virtual machine must be powered on.
Turn on time synchronization	Turns on time synchronization between the virtual machine and the ESX server in VMware Tools.
Unmount VMware tools installer	Unmounts the VMware Tools CD-ROM.
Upgrade VMware tools	Upgrades VMware Tools on a virtual machine.
Upgrade VMware tools at next reboot	Upgrades VMware Tools on a virtual machine without performing an automatic reboot.

About Headless Systems

ESXi supports the detection and configuration of headless systems.

A headless system is a system that can be operated without a monitor, keyboard, or mouse. Network Appliance boxes do not have VGA, the primary interface is a single serial port. You can set up your existing headless systems to use ESXi. You can add ESXi appliances to a data center where virtual machines are managed with vSphere Virtual Center. All existing ESXi features can be used with a headless system that is configured with either embedded flash or minimal local storage. ESXi allows for dynamic switching between different serial modes, which is useful for diagnosing and debugging problems. You can switch between modes to view or modify system parameters.

How to Detect a Headless System

ESXi automatically detects headless systems.

ESXi automatically redirects the DCUI over a serial port connection to improve headless detection. When ESXi automatically detects a headless system, ESXi will set up the serial port as COM1, 115200 baud, and redirects the DCUI over this serial port. The specific settings of com port and baud rate are read from the Serial Port Console Redirection (SPCR) table, if it exists. This behavior can be deactivated using new boot parameters if the default settings are not acceptable. You can set the `headless` flag in the ACPI FADT table to mark a system as headless.

About Serial Mode Dynamic Switching

ESXi supports dynamic switching between four different serial port modes.

ESXi supports serial mode dynamic switching to provide maximum platform flexibility, and to allow debugging and supportability in the text box. ESXi examines the input characters for any serial port mode and switches the modes based on the input key sequence. DCUI, Shell, GDB, and Logging modes are supported. If you have two serial ports, only one of the four modes is allowed on each port. Two serial ports cannot be in the same mode. If you attempt a dynamic switch to a mode in use by the other serial port, the request is ignored. Dynamic switching eliminates the need to interrupt the boot process manually or to create a custom image to redirect to a serial port. It also addresses supportability issues regarding headless systems that only have one serial port, by making it possible to switch the serial port between different modes of operation.

ESXi Serial Port Modes

ESXi supports four serial port modes.

There are four serial port modes in ESXi:

Logging mode – Logging mode is the default mode in a debug build. Logging mode sends the vmkernel.log over the serial port.

GDB mode – Use GDB mode for dedicated debugging.

Shell mode – Shell mode is the shell port access, which is similar to SSH.

DCUI mode – DCUI mode is a Direct Console User Interface. This is the user interface that is displayed when you boot ESXi using a monitor.

Note:

Only COM1 and COM2 ports are supported. USB serial or PCI serial cards are not supported.

Dynamic Switching Keystrokes

ESXi includes a unique keystroke sequence that allows dynamic serial mode switching.

Dynamic Switching Keystrokes

Once the correct keystroke sequence is entered, the system switches the serial port to the desired mode.

Logging mode: `Ctrl+G, Ctrl+B, 1`

Shell mode: `Ctrl+G, Ctrl+B, 2`

DCUI mode: `Ctrl+G, Ctrl+B, 3`

GDB mode: `Ctrl+G, Ctrl+B, ?`

Note: Once in GDB mode, you cannot switch modes again using a key sequence. You must use the CLI to switch modes.

Serial Port Dynamic Switching Using the CLI

You can switch serial modes using the CLI.

Dynamic Switching Using the CLI

Use esxcfg-advcfg to set the current mode to **none**. Then set the new desired mode using the CLI.

Logging mode: `esxcfg-advcfg -s com1 /Misc/LogPort`

Shell mode: `esxcfg-advcfg -s com1 /Misc/ShellPort`

DCUI mode: `esxcfg-advcfg -s com1 /Misc/ConsolePort`

GDB mode: `esxcfg-advcfg -s com1 /Misc/GDBPort`

Example

If the serial mode is set to logging mode, enter these two commands to switch it to DCUI mode.

```
§. > esxcfg-advcfg –s none /Misc/LogPort
§. > esxcfg-advcfg –s com1 /Misc/ConsolePort
```

Controlling the Serial DCUI

You can use alternate keystrokes to control the DCUI over a serial port. These alternate are useful when F2 or other function keys cannot be used.

Controlling the Serial DCUI

Alternate keystroke mappings for DCUI mode:

- Esc + 1 -> F1

- Esc + 2 -> F2
- Esc + 3 -> F3
- Esc + 4 -> F4
- Esc + 5 -> F5
- Esc + 6 -> F6
- Esc + 7 -> F7
- Esc + 8 -> F8
- Esc + 9 -> F9
- Esc + 0 -> F10
- Esc + ! -> F11
- Esc + @ -> F12

Troubleshooting Overview

vSphere Troubleshooting contains common troubleshooting scenarios and provides solutions for each of these problems. You can also find guidance here for resolving problems that have similar origins. For unique problems, consider developing and adopting a troubleshooting methodology.

The following approach for effective troubleshooting elaborates on how to gather troubleshooting information, such as identifying symptoms and defining the problem space. Troubleshooting with log files is also discussed.

Troubleshooting vCenter Server

These troubleshooting topics provide solutions to problems you might encounter in vCenter Server.

Guidelines for Troubleshooting

To troubleshoot your implementation of vSphere, identify the symptoms of the problem, determine which of the components are affected, and test possible solutions.

Identifying Symptoms	A number of potential causes might lead to the under-performance or nonperformance of your implementation. The first step in efficient troubleshooting is to identify exactly what is going wrong.
Defining the Problem Space	After you have isolated the symptoms of the problem, you must define the problem space. Identify the software or hardware components that are affected and might be causing the problem and those components that are not involved.
Testing Possible Solutions	When you know what the symptoms of the problem are and which components are involved, test the solutions systematically until the problem is resolved.

Identifying Symptoms

Before you attempt to resolve a problem in your implementation, you must identify precisely how it is failing.

The first step in the troubleshooting process is to gather information that defines the specific symptoms of what is happening. You might ask these questions when gathering this information:

- What is the task or expected behavior that is not occurring?
- Can the affected task be divided into subtasks that you can evaluate separately?
- Is the task ending in an error? Is an error message associated with it?
- Is the task completing but in an unacceptably long time?

- Is the failure consistent or sporadic?
- What has changed recently in the software or hardware that might be related to the failure?

Defining the Problem Space

After you identify the symptoms of the problem, determine which components in your setup are affected, which components might be causing the problem, and which components are not involved.

To define the problem space in an implementation of vSphere, be aware of the components present. In addition to VMware software, consider third-party software in use and which hardware is being used with the VMware virtual hardware.

Recognizing the characteristics of the software and hardware elements and how they can impact the problem, you can explore general problems that might be causing the symptoms.

- Misconfiguration of software settings
- Failure of physical hardware
- Incompatibility of components

Break down the process and consider each piece and the likelihood of its involvement separately. For example, a case that is related to a virtual disk on local storage is probably unrelated to third-party router configuration. However, a local disk controller setting might be contributing to the problem. If a component is unrelated to the specific symptoms, you can probably eliminate it as a candidate for solution testing.

Think about what changed in the configuration recently before the problems started. Look for what is common in the problem. If several problems started at the same time, you can probably trace all the problems to the same cause.

Testing Possible Solutions

After you know the problem's symptoms and which software or hardware components are most likely involved, you can systematically test solutions until you resolve the problem.

With the information that you have gained about the symptoms and affected components, you can design tests for pinpointing and resolving the problem. These tips might make this process more effective.

- Generate ideas for as many potential solutions as you can.
- Verify that each solution determines unequivocally whether the problem is fixed. Test each potential solution but move on promptly if the fix does not resolve the problem.
- Develop and pursue a hierarchy of potential solutions based on likelihood. Systematically eliminate each potential problem from the most likely to the least likely until the symptoms disappear.
- When testing potential solutions, change only one thing at a time. If your setup works after many things are changed at once, you might not be able to discern which of those things made a difference.
- If the changes that you made for a solution do not help resolve the problem, return the implementation to its previous status. If you do not return the implementation to its previous status, new errors might be introduced.
- Find a similar implementation that is working and test it in parallel with the implementation that is not working properly. Make changes on both systems at the same time until few differences or only one difference remains between them.

Troubleshooting with vCenter Server Logs

You can often obtain valuable troubleshooting information by looking at the logs provided by the various services and agents that your implementation is using.

Most logs are located in `/var/log/vmware/<service_name>` for vCenter Server deployments.

Common Logs

The following logs are common to all vCenter Server deployments.

Table 150: Common Log Directories

Log Directory	Description
`../firstboot`	Stores first boot logs
`applmgmt` and `applmgmt-audit`	Stores logs related to the VMware Appliance Management Service
`cloudvm`	Stores logs for allotment and distribution of resources between services
`rhttpproxy`	Stores logs for the VMware HTTP Reverse Proxy service
`sca`	Stores logs for the VMware Service Control Agent service
`vapi`	Stores logs for the VMware vAPI Endpoint service
`vmafdd`	Stores logs for the VMware Authentication Framework - LDAP service
`vmdird`	Stores logs for the VMware Directory Service - LDAP service
`vmon`	Stores logs for the VMware Service Lifecycle Manager service

Management Node Logs

The following logs are available if a management node deployment is selected.

Table 151: Management Node Log Directories

Log Directory	Service
`rbd`	VMware vSphere Auto Deploy
`content-library`	VMware Content Library Service
`eam`	VMware ESX Agent Manager
`netdumper`	VMware vSphere ESXi Dump Collector
`perfcharts`	VMware Performance Charts Service
`vmcam`	VMware vSphere Authentication Proxy
`vmdird`	VMware Directory Service - LDAP
`vmware-sps`	VMware vSphere Profile-Driven Storage Service
`vpxd`	VMware vCenter Server
`vpostgres`	VMware Postgres service
`vcha`	VMware vCenter High Availability service

Troubleshooting vCenter Server and ESXi Host Certificates

Certificates are automatically generated when you install vCenter Server. These default certificates are not signed by a commercial certificate authority (CA) and might not provide strong security. You can replace default vCenter Server certificates with certificates signed by a commercial CA. When you replace vCenter Server and ESXi certificates, you might encounter errors.

New vCenter Server Certificate Does Not Appear to Load

After you replace default vCenter Server certificates, the new certificates might not appear to load.

When you install new vCenter Server certificates, you might not see the new certificate.

Existing open connections to vCenter Server are not forcibly closed and might still use the old certificate.

To force all connections to use the new certificate, use one of the following methods.

- Restart the network stack or network interfaces on the server.
- Restart the vCenter Server service.

vCenter Server Cannot Connect to Managed Hosts

After you replace default vCenter Server certificates and restart the system, vCenter Server might not be able to connect to managed hosts.

vCenter Server cannot connect to managed hosts after server certificates are replaced and the system is restarted.

Log into the host as the root user and reconnect the host to vCenter Server.

Troubleshooting Hosts

The host troubleshooting topics provide solutions to potential problems that you might encounter when using your vCenter Servers and ESXi hosts.

Troubleshooting vSphere HA Host States

vCenter Server reports vSphere HA host states that indicate an error condition on the host. Such errors can prevent vSphere HA from fully protecting the virtual machines on the host and can impede vSphere HA's ability to restart virtual machines after a failure. Errors can occur when vSphere HA is being configured or unconfigured on a host or, more rarely, during normal operation. When this happens, you should determine how to resolve the error, so that vSphere HA is fully operational.

vSphere HA Agent Is in the Agent Unreachable State

The vSphere HA agent on a host is in the Agent Unreachable state for a minute or more. User intervention might be required to resolve this situation.

vSphere HA reports that an agent is in the Agent Unreachable state when the agent for the host cannot be contacted by the primary host or by vCenter Server. Consequently, vSphere HA is not able to monitor the virtual machines on the host and might not restart them after a failure.

A vSphere HA agent can be in the Agent Unreachable state for several reasons. This condition most often indicates that a networking problem is preventing vCenter Server or the primary host from contacting the agent on the host, or that all hosts in the cluster have failed. This condition can also indicate the unlikely situation that vSphere HA was deactivated and then reactivated on the cluster while vCenter Server could not communicate with the vSphere HA agent on the host, or that the ESXi host agent on the host has failed, and the watchdog process was unable to restart it. In any of these cases, a failover event is not triggered when a host goes into the Unreachable state.

Determine if vCenter Server is reporting the host as not responding. If so, there is a networking problem, an ESXi host agent failure, or a total cluster failure. After the condition is resolved, vSphere HA should work correctly. If not, reconfigure vSphere HA on the host. Similarly, if vCenter Server reports the hosts are responding but a host's state is Agent Unreachable, reconfigure vSphere HA on that host.

vSphere HA Agent is in the Uninitialized State

The vSphere HA agent on a host is in the Uninitialized state for a minute or more. User intervention might be required to resolve this situation.

vSphere HA reports that an agent is in the Uninitialized state when the agent for the host is unable to enter the run state and become the primary host or to connect to the primary host. Consequently, vSphere HA is not able to monitor the virtual machines on the host and might not restart them after a failure.

A vSphere HA agent can be in the Uninitialized state for one or more reasons. This condition most often indicates that the host does not have access to any datastores. Less frequently, this condition indicates that the host does not have access to its local datastore on which vSphere HA caches state information, the agent on the host is inaccessible, or the vSphere HA agent is unable to open required firewall ports. It is also possible that the ESXi host agent has stopped.

Search the list of the host's events for recent occurrences of the event `vSphere HA Agent for the host has an error`. This event indicates the reason for the host being in the uninitialized state. If the condition exists because of a datastore problem, resolve whatever is preventing the host from accessing the affected datastores. If the ESXi host agent has stopped, you must restart it. After the problem has been resolved, if the agent does not return to an operational state, reconfigure vSphere HA on the host.

Note: If the condition exists because of a firewall problem, check if there is another service on the host that is using port 8182. If so, shut down that service, and reconfigure vSphere HA.

vSphere HA Agent is in the Initialization Error State

The vSphere HA agent on a host is in the Initialization Error state for a minute or more. User intervention is required to resolve this situation.

vSphere HA reports that an agent is in the Initialization Error state when the last attempt to configure vSphere HA for the host failed. vSphere HA does not monitor the virtual machines on such a host and might not restart them after a failure.

This condition most often indicates that vCenter Server was unable to connect to the host while the vSphere HA agent was being installed or configured on the host. This condition might also indicate that the installation and configuration completed, but the agent did not become a primary host or a secondary host within a timeout period. Less frequently, the condition is an indication that there is insufficient disk space on the host's local datastore to install the agent, or that there are insufficient unreserved memory resources on the host for the agent resource pool. Finally, for ESXi 5.x hosts, the configuration fails if a previous installation of another component required a host reboot, but the reboot has not yet occurred.

When a Configure HA task fails, a reason for the failure is reported.

Reason for Failure	Action
Host communication errors	Resolve any communication problems with the host and retry the configuration operation.
Timeout errors	Possible causes include that the host crashed during the configuration task, the agent failed to start after being installed, or the agent was unable to initialize itself after starting up. Verify that vCenter Server is able to communicate with the host. If so, see vSphere HA Agent Is in the Agent Unreachable State or vSphere HA Agent is in the Uninitialized State for possible solutions.
Lack of resources	Free up approximately 75MB of disk space. If the failure is due to insufficient unreserved memory, free up memory on the host by either relocating virtual machines to another host or reducing their reservations. In either case, retry the vSphere HA configuration task after resolving the problem.

Reason for Failure	Action
Reboot pending	If an installation for a 5.0 or later host fails because a reboot is pending, reboot the host and retry the vSphere HA configuration task.

vSphere HA Agent is in the Uninitialization Error State

The vSphere HA agent on a host is in the Uninitialization Error state. User intervention is required to resolve this situation.

vSphere HA reports that an agent is in the Uninitialization Error state when vCenter Server is unable to unconfigure the agent on the host during the Unconfigure HA task. An agent left in this state can interfere with the operation of the cluster. For example, the agent on the host might elect itself as primary host and lock a datastore. Locking a datastore prevents the valid cluster primary host from managing the virtual machines with configuration files on that datastore.

This condition usually indicates that vCenter Server lost the connection to the host while the agent was being unconfigured.

Add the host back to vCenter Server (version 5.0 or later). The host can be added as a stand-alone host or added to any cluster.

vSphere HA Agent is in the Host Failed State

The vSphere HA agent on a host is in the Host Failed state. User intervention is required to resolve the situation.

Usually, such reports indicate that a host has actually failed, but failure reports can sometimes be incorrect. A failed host reduces the available capacity in the cluster and, in the case of an incorrect report, prevents vSphere HA from protecting the virtual machines running on the host.

This host state is reported when the vSphere HA primary host to which vCenter Server is connected is unable to communicate with the host and with the heartbeat datastores that are in use for the host. Any storage failure that makes the datastores inaccessible to hosts can cause this condition if accompanied by a network failure.

Check for the noted failure conditions and resolve any that are found.

vSphere HA Agent is in the Network Partitioned State

The vSphere HA agent on a host is in the Network Partitioned state. User intervention might be required to resolve this situation.

While the virtual machines running on the host continue to be monitored by the primary hosts that are responsible for them, vSphere HA's ability to restart the virtual machines after a failure is affected. First, each primary host has access to a subset of the hosts, so less failover capacity is available to each host. Second, vSphere HA might be unable to restart a FT Secondary VM after a failure. See also *vSphere Availability* troubleshooting.

A host is reported as partitioned if both of the following conditions are met:

- The vSphere HA primary host to which vCenter Server is connected is unable to communicate with the host by using the management (or VMware vSAN™)network, but is able to communicate with that host by using the heartbeat datastores that have been selected for it.
- The host is not isolated.

A network partition can occur for a number of reasons including incorrect VLAN tagging, the failure of a physical NIC or switch, configuring a cluster with some hosts that use only IPv4 and others that use only IPv6, or the management networks for some hosts were moved to a different virtual switch without first putting the host into maintenance mode.

Resolve the networking problem that prevents the hosts from communicating by using the management networks.

vSphere HA Agent is in the Network Isolated State

The vSphere HA agent on a host is in the Network Isolated state. User intervention is required to resolve this situation.

When a host is in the Network Isolated state, there are two things to consider -- the isolated host and the vSphere HA agent that holds the primary role.

- On the isolated host, the vSphere HA agent applies the configured isolation response to the running VMs, determining if they should be shut down or powered off. It does this after checking whether a primary agent is able to take responsibility for each VM (by locking the VM's home datastore.) If not, the agent defers applying the isolation response for the VM and rechecks the datastore state after a short delay.
- If the vSphere HA primary agent can access one or more of the datastores, it monitors the VMs that were running on the host when it became isolated and attempts to restart any that were powered off or shut down.

A host is network isolated if both of the following conditions are met:

- Isolation addresses have been configured and the host is unable to ping them.
- The vSphere HA agent on the host is unable to access any of the agents running on the other cluster hosts.

Note: If your vSphere HA cluster has vSAN enabled, a host is determined to be isolated if it cannot communicate with the other vSphere HA agents in the cluster and cannot reach the configured isolation addresses. Although the vSphere HA agents use the vSAN network for inter-agent communication, the default isolation address is still the gateway of the host. Hence, in the default configuration, both networks must fail for a host be declared isolated.

Resolve the networking problem that is preventing the host from pinging its isolation addresses and communicating with other hosts.

Configuration of vSphere HA on Hosts Times Out

The configuration of a vSphere HA cluster might time out on some of the hosts added to it.

When you enable vSphere HA on an existing cluster with a large number of hosts and virtual machines, the setup of vSphere HA on some of the hosts might fail.

This failure is the result of a time out occurring before the installation of vSphere HA on the host(s) completes.

Set the vCenter Server advanced option config.vpxd.das.electionWaitTimeSec to value=240. Once this change is made, the time outs do not occur.

Authentication Token Manipulation Error

Creating a password that does not meet the authentication requirements of the host causes an error.

When you create a password on the host, the following fault message appears: `A general system error occurred: passwd: Authentication token manipulation error`.

The following message is included: `Failed to set the password. It is possible that your password does not meet the complexity criteria set by the system.`

The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so`. If the password is not compliant, the error appears.

When you create a password, include a mix of characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters such as an underscore or dash.

Your user password must meet the following length requirements.

- Passwords containing characters from three character classes must be at least eight characters long.
- Passwords containing characters from all four character classes must be at least seven characters long.

Note: An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

For more information, see the *vSphere Security* documentation.

Unable to Download VIBs When Using vCenter Server Reverse Proxy

You are unable to download VIBs if vCenter Server is using a custom port for the reverse proxy.

If you configure vCenter Server reverse proxy to use a custom port, the VIB downloads fail.

If vCenter Server is using a custom port for the reverse proxy, the custom port is not automatically enabled in the ESXi firewall and the VIB downloads fail.

1. Open an SSH connection to the host and log in as root.
2. Optional: List the existing firewall rules.

   ```
   esxcli network firewall ruleset list
   ```

3. Optional: Back up the `/etc/vmware/firewall/service.xml` file.

   ```
   cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
   ```

4. Edit the access permissions of the `service.xml` file to allow writes by running the `chmod` command.
   - To allow writes, run `chmod644 /etc/vmware/firewall/service.xml`.
   - To toggle the sticky bit flag, run `chmod+t  /etc/vmware/firewall/service.xml`.
5. Open the `service.xml` file in a text editor.
6. Add a new rule to the `service.xml` file that enables the custom port for the vCenter Server reverse proxy .

   ```
   <service id='id_value'>
      <id>vcenterrhttpproxy</id>
      <rule id='0000'>
        <direction>outbound</direction>
        <protocol>tcp</protocol>
        <port type='dst'>custom_reverse_proxy_port</port>
      </rule>
      <enabled>true</enabled>
      <required>false</required>
   </service>
   ```

   Where *`id_value`* must be a unique value, for example, if the last listed service in the `service.xml` file has ID 0040, you must enter id number 0041.
7. Revert the access permissions of the `service.xml` file to the default read-only setting.

   ```
   chmod 444 /etc/vmware/firewall/service.xml
   ```

8. Refresh the firewall rules for the changes to take effect.

   ```
   esxcli network firewall refresh
   ```

9. Optional: List the updated rule set to confirm the change.

   ```
    esxcli network firewall ruleset list
   ```

10. Optional: If you want the firewall configuration to persist after a reboot of the ESXi host, copy the `service.xml` onto persistent storage and modify the `local.sh` file.
    a) Copy the modified `service.xml` file onto persistent storage, for example `/store/`, or onto a VMFS volume, for example `/vmfs/volumes/volume/`.

    ```
    cp /etc/vmware/firewall/service.xml location_of_xml_file
    ```

    You can store a VMFS volume in a single location and copy it to multiple hosts.
    b) Add the `service.xml` file information to the `local.sh` file on the host.

    ```
    cp location_of_xml_file /etc/vmware/firewall
    esxcli network firewall refresh
    ```

    Where *location_of_xml_file* is the location to which the file was copied.

Troubleshooting Licensing

The troubleshooting licensing topics provide solutions to problems that you might encounter as a result of an incorrect or incompatible license setup in vSphere.

Troubleshooting Host Licensing

You might encounter different problems that result from an incompatible or incorrect license configuration of ESXi hosts.

Unable to Assign a License to an ESXi Host

Under certain conditions, you might be unable to assign a license to an ESXi host.

You try to assign a license to an ESXi host, but you cannot perform the operation and you receive an error message.

You might be unable to assign a license to an ESXi host because of the following reasons:

- The calculated license usage for the host exceeds the license capacity. For example, you have a vSphere license key with capacity for two CPUs. You try to assign the key to a host that has four CPUs. You cannot assign the license, because the required license usage for the host is greater than the license capacity.
- The features on the host do not match the license edition. For example, you might configure hosts with vSphere Distributed Switch and vSphere DRS while in evaluation mode. Later, you try to assign vSphere Standard license to the hosts. This operation fails because the vSphere Standard edition does not include vSphere Distributed Switch and vSphere DRS.
- The host is connected to a vCenter Server system that is assigned a license that restricts the edition of the license that you want to assign.

- Assign a license with larger capacity.
- Upgrade the license edition to match the resources and features on the host, or deactivate the features that do not match the license edition.
- Assign a vSphere license whose edition is compatible with the license edition of vCenter Server.

ESXi Host Disconnects from vCenter Server

An ESXi host might disconnect from vCenter Server or all ESXi hosts might disconnect from vCenter Server at the same time.

An ESXi host disconnects from vCenter Server when the host evaluation period or license expires. All ESXi hosts disconnect from vCenter Server when the evaluation period or the license of vCenter Server expire. You receive a licensing-related error message both when a single host disconnects and when all hosts disconnect. You cannot add hosts to the vCenter Server inventory. The hosts and the virtual machines on the hosts continue to run.

- The 60-day evaluation period of the host has expired or the host license has expired.
- The 60-day evaluation period of vCenter Server is expired or the vCenter Server license is expired.

- Assign a vSphere license to the ESXi host and try to reconnect it to vCenter Server.
- Assign a vCenter Server license to the vCenter Server system.

Unable to Power On a Virtual Machine

You try to power on a virtual machine, but the operation is unsuccessful and you receive an error message.

You cannot power on a virtual machine on an ESXi host.

You might be unable to power on a virtual machine because of the following reasons.

- The 60-day evaluation period of the host is expired.
- The license of the host is expired.

Table 152: Power on a Virtual Machine

Cause	Solution
The evaluation period of the host is expired	Assign a vSphere license to the ESXi host
The license of the host is expired	Assign a vSphere license to the ESXi host

Unable to Configure or Use a Feature

You cannot use a feature or change its configuration.

You cannot use or configure a feature and a licensing-related error message appears.

The ESXi host or the vCenter Server system is assigned a license that does not support the features that you want to configure.

Check the licensed features on the ESXi host and on the vCenter Server system. Upgrade the edition of the license assigned to the host or vCenter Server if they do not include the features that you try to configure or use.

vSphere Virtual Machine Administration Guide

vSphere Virtual Machine Administration describes how to create, configure, and manage virtual machines in the VMware vSphere® environment.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we have updated this guide to remove instances of non-inclusive language.

This guide provides introductions to the tasks that you can perform within the system and also cross-references to the documentation that describes the tasks in detail.

This information focuses on managing virtual machines and includes the following information.

- Creating and deploying virtual machines, templates, and clones
- Deploying OVF templates
- Using content libraries to manage templates and other library items
- Configuring virtual machine hardware and virtual machine options
- Managing multi-tiered applications with VMware vSphere vApp
- Monitoring solutions with the vCenter Solutions Manager
- Managing virtual machines, including using snapshots
- Upgrading virtual machines
- Troubleshooting virtual machines

vSphere Virtual Machine Administration covers VMware ESXi™ and VMware vCenter Server®.

Intended Audience

This information is written for experienced Windows or Linux system administrators who are familiar with virtualization.

Introduction to VMware vSphere Virtual Machines

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine consists of a set of specification and configuration files and is backed by the physical resources of a host. Every virtual machine has virtual devices that provide the same functionality as physical hardware but are more portable, more secure, and easier to manage.

Before you start creating and managing virtual machines, you benefit from some background information, for example, the virtual machine files, life cycle, components, and so on.

Virtual Machine Files

A virtual machine consists of several files that are stored on a storage device. The key files are the configuration file, virtual disk file, NVRAM setting file, and log file. You configure virtual machine settings through the vSphere Client, ESXCLI, or the vSphere Web Services SDK.

CAUTION: Do not change, move, or delete virtual machine files without instructions from a VMware Technical Support representative.

Table 153: Virtual Machine Files

File	Usage	Description
`.vmx`	*`vmname`*`.vmx`	Virtual machine configuration file

File	Usage	Description
.vmxf	*vmname*.vmxf	Additional virtual machine configuration files
.vmdk	*vmname*.vmdk	Virtual disk characteristics
-flat.vmdk	*vmname*-flat.vmdk	Virtual machine data disk
.nvram	*vmname*.nvram or nvram	Virtual machine BIOS or EFI configuration
.vmem	*vmname*.vmem	Virtual machine paging backup file
.vmsd	*vmname*.vmsd	Virtual machine snapshots information (metadata) file
.vmsn	*vmname*.vmsn	Virtual machine memory snapshot file
.vswp	*vmname*.vswp	Virtual machine swap file
.vmss	*vmname*.vmss	Virtual machine suspend file
.log	vmware.log	Current virtual machine log file
-#.log	vmware-#.log (where # is a number starting with 1)	Old virtual machine log files

Additional files are created when you perform certain tasks with the virtual machine.

- A .hlog file is a log file that is used by vCenter Server to keep track of virtual machine files that must be removed after a certain operation completes.
- A .vmtx file is created when you convert a virtual machine to a template. The .vmtx file replaces the virtual machine configuration file (.vmx file).

Virtual Machines and the Virtual Infrastructure

The infrastructure that supports virtual machines consists of at least two software layers, virtualization and management. In vSphere, ESXi provides the virtualization capabilities that aggregate and present the host hardware to virtual machines as a normalized set of resources. Virtual machines run on ESXi hosts that vCenter Server manages.

vCenter Server can pool the resources of multiple hosts and lets you effectively monitor and manage your data center infrastructure. You can manage resources for virtual machines, provision virtual machines, schedule tasks, collect statistics logs, create templates, and more. vCenter Server also provides vSphere vMotion™, vSphere Storage vMotion, vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), and vSphere Fault Tolerance. These services enable efficient and automated resource management and high availability for virtual machines.

The vSphere Client is the primary interface for managing vCenter Server, ESXi hosts, and virtual machines. The vSphere Client also provides console access to virtual machines.

In the vCenter Server hierarchy that you see in the vSphere Client, a data center is the top-level container of ESXi hosts, folders, clusters, resource pools, vSphere vApps, virtual machines, and so on.

Datastores are virtual representations of underlying physical storage resources. Datastores hide the idiosyncrasies of the underlying physical storage and present a uniform model for the storage resources required by virtual machines. A datastore is the storage location (for example, a physical disk or LUN on a RAID, or a SAN) for virtual machine files.

Virtual Machine Lifecycle

You have many options for creating and deploying virtual machines. You can create a single virtual machine and install a guest operating system and VMware Tools on it. You can clone an existing virtual machine or convert it to a template. You can also deploy OVF or OVA templates.

The vSphere Client**New Virtual Machine** wizard and the **Edit Settings** dialog box let you add, configure, or remove most of the virtual machine's hardware, options, and resources. You monitor CPU, memory, disk, network, and storage metrics through the performance charts in the vSphere Client. Snapshots let you capture the state of the virtual machine,

including the virtual machine memory, settings, and virtual disks. You can roll back to the previous virtual machine state when needed.

With vSphere vApps, you can manage multi-tiered applications. You use vSphere Lifecycle Manager to perform orchestrated upgrades to upgrade the virtual hardware and VMware Tools of virtual machines in the inventory at the same time.

When a virtual machine is no longer needed, you can remove it from the inventory without deleting it from the datastore, or you can delete the virtual machine and all its files.

Virtual Machine Components

Virtual machines typically have an operating system, VMware Tools, and virtual resources and hardware. You manage these components like you manage the components of a physical computer.

Operating System	You install a guest operating system on a virtual machine the same way you install an operating system on a physical computer. You must have a CD/DVD-ROM or ISO image containing the installation files from an operating system vendor. After installation, you are responsible for securing and patching the operating system.
VMware Tools	VMware Tools is a suite of utilities that enhances the performance of the virtual machine guest operating system and improves management of the virtual machine. It includes device drivers and other software that is essential for your VM. With VMware Tools, you have more control over the virtual machine interface.
Compatibility Setting	In the vSphere Client, you assign each virtual machine to a compatible ESXi host version, cluster, or data center by applying a compatibility setting. The compatibility setting determines which ESXi host versions the virtual machine can run on and the hardware features available to the virtual machine.
Hardware Devices	Each virtual hardware device performs the same function for the virtual machine as hardware on a physical computer does. Every virtual machine has CPU, memory, and disk resources. CPU virtualization emphasizes performance and runs directly on the processor whenever possible. The underlying physical resources are used whenever possible. The virtualization layer runs instructions only as needed to make virtual machines operate as if they were running directly on a physical machine. All recent operating systems provide support for virtual memory, allowing software to use more memory than the machine physically has. Similarly, the ESXi hypervisor provides support for overcommitting virtual machine memory, where the amount of guest memory configured for all virtual machines might be larger than the amount of the host's physical memory. You access the hardware devices in the **Edit Settings** dialog box. Not all devices are configurable. Some hardware devices are part of the virtual motherboard and appear in the expanded device list of the **Edit Settings** dialog box, but you cannot modify or remove them. For a list of hardware devices and their functions, see Virtual Machine Hardware Available to vSphere Virtual Machines. In the **Edit Settings** dialog box you can also add virtual hardware devices to the virtual machine. You can use the memory or CPU hotplug options to add memory or CPU resources to a virtual machine while the virtual machine is running. You can deactivate Memory or CPU hotplug to avoid adding memory or CPUs while the virtual machine is running. Memory hotplug is supported on

all 64 bit operating systems, but to use the added memory, the guest operating system must also support this feature. See the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility

Virtual Machine Hardware Available to vSphere Virtual Machines

VMware provides devices, resources, profiles, and vServices that you can configure or add to your virtual machine.

Table 154: Virtual Machine Hardware and Descriptions

Hardware Device	Description
CPU	You can configure a virtual machine that runs on an ESXi host to have one or more virtual processors. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host.
Chipset	The motherboard uses VMware proprietary devices based on the following chips: • Intel 440BX AGPset 82443BX Host Bridge/Controller • Intel 82371AB (PIIX4) PCI ISA IDE Xcelerator • National Semiconductor PC87338 ACPI 1.0 and PC98/99 Compliant SuperI/O • Intel 82093AA I/O Advanced Programmable Interrupt Controller
DVD/CD-ROM Drive	Installed by default when you create a virtual machine. You can configure DVD/CD-ROM devices to connect to client devices, host devices, or datastore ISO files. You can add, remove, or configure DVD/CD-ROM devices.
Hard Disk	Stores the operating system of a virtual machine, program files, and other data associated with its activities. A virtual disk is a large physical file, or a set of files, that can be copied, moved, archived, and backed up as easily as any other file.
IDE 0, IDE 1	By default, two Integrated Drive Electronics (IDE) interfaces are presented to the virtual machine. The IDE interface (controller) is a standard way for storage devices (floppy drives, hard drives, and CD-ROM drives) to connect to the virtual machine.
Keyboard	Provides keyboard input from any virtual machine consoles.
Memory	The virtual hardware memory size determines how much memory applications that are running inside the virtual machine have available to them. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size.
Network Adapter	ESXi networking features provide communication between virtual machines on the same host, between virtual machines on different hosts, and between other virtual and physical machines. When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.
Parallel port	Interface for connecting peripherals to the virtual machine. The virtual parallel port can connect to a file. You can add, remove, or configure virtual parallel ports.
PCI controller	Bus on the virtual machine motherboard that communicates with components such as hard disks and other devices. One PCI controller is presented to the virtual machine. You cannot configure or remove this device.
PCI Device	You can add up to 16 PCI vSphere DirectPath devices to a virtual machine. The devices must be reserved for PCI passthrough on the host on which the virtual machine runs. Snapshots are not supported with DirectPath I/O passthrough devices.
Pointing device	Mirrors the pointing device that is connected to the virtual machine console when you first connect to the console.

Hardware Device	Description
Serial Port	Interface for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port, to a file on the host computer, or over the network. You can also use it to establish a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. You can configure a virtual machine with up to 32 serial ports. You can add, remove, or configure virtual serial ports.
SATA controller	Provides access to virtual disks and DVD/CD-ROM devices. The SATA virtual controller appears to a virtual machine as an AHCI SATA Controller.
SCSI controller	Provides access to virtual disks. The SCSI virtual controller appears to a virtual machine as different types of controllers, including LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual. You can change the SCSI controller type, allocate bus sharing for a virtual machine, or add a paravirtualized SCSI controller.
SIO controller	Provides serial and parallel ports, floppy devices, and performs system management activities. One SIO controller is available to the virtual machine. You cannot configure or remove this device.
USB controller	The USB hardware chip that provides USB 1.x and USB 2.0 function to the USB ports that it manages. The virtual USB Controller is the software virtualization of the USB 1.x and USB 2.0 host controller function in the virtual machine.
USB xHCI controller	The USB hardware chip that provides USB 3 function to the USB ports that it manages. The virtual USB xHCI controller is the software virtualization of the USB 3 host controller function in the virtual machine.
USB device	
VMCI	Virtual Machine Communication Interface device. Provides a high-speed communication channel between a virtual machine and the hypervisor. You cannot add or remove VMCI devices.
NVMe controller	NVM Express controller. NVMe is a logical device interface specification for accessing nonvolatile storage media attached through a PCI Express (PCIe) bus in real and virtual hardware.
NVDIMM controller	Provides access to the non-volatile memory resources of the host.
NVDIMM device	Non-Volatile Dual In-Line Memory Module. NVDIMM modules are memory devices that sit on an ordinary memory channel, but contain non-volatile memory. You can add up to 64 virtual NVDIMM devices to a virtual machine.
TPM device	Trusted Platform Module. When you add a virtual TPM 2.0 device to a virtual machine, the guest OS uses the device to store sensitive information, perform cryptographic tasks, or attest the integrity of the guest platform.
Virtual Precision Clock device	A virtual clock device that provides a virtual machine with access to the system time of the primary ESXi host.
Virtual Watchdog Timer device	To ensure self-reliance related to the system performance within a virtual machine. If the guest operating system stops responding and cannot recover on its own due to software glitches or errors, the watchdog timer waits for a predefined period of time and then restarts the system.
vSGX device	Virtual Intel® Software Guard Extensions (vSGX) provides a virtual machine additional security to your workloads. Intel SGX is a processor-specific technology that defines private regions of memory, called enclaves. Intel SGX protects the enclave contents from disclosure and modification in such a way that code running outside the enclave cannot access them.
RDM disk	You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file.
PS2 controller	PS2 controller provides access to the virtual keyboard and point to the PS2 interface.

Hardware Device	Description
Video card	A virtual graphics card that provides graphics acceleration and display capabilities for virtual machine consoles.

Virtual Machine Options

Use the available virtual machine options to fine-tune the settings and behavior of your virtual machine and to ensure maximum performance.

A virtual machine might be running in any of several locations, such as ESXi hosts, data centers, clusters, or resource pools. Many of the options and resources that you configure have dependencies on and relationships with these objects.

VMware virtual machines have the following options.

General Options	View or modify the virtual machine name, and check the location of the configuration file and the working location of the virtual machine.
Encryption Options	Enable or deactivate encryption for the virtual machine if the vCenter Server instance is in a trusted relationship with a KMS server. For more information, see the *vSphere Security* documentation. You can also enable or deactivate encrypted vMotion for virtual machines that are not encrypted. You can set encrypted vMotion to the deactivated, opportunistic, or required state. You can enable encrypted vMotion during virtual machine creation. Alternatively, you can change the encrypted vMotion state later. For more information, see the *vCenter Server and Host Management* documentation.
Power Management	Manage guest power options. Suspend the virtual machine or leave the virtual machine powered on when you put the guest operating system into standby.
VMware Tools	Manage the power controls for the virtual machine, run VMware Tools scripts, and upgrade VMware Tools during power cycling. Automatically synchronize the time between guest and host operating systems, and periodically synchronize the guest time with the host if the virtual machine guest operating system does not have a native time synchronization software.
Virtualization Based Security (VBS)	Enable VBS to provide an additional level of protection to the virtual machine. VBS is available on the latest Windows OS versions. For more information, see the *vSphere Security* documentation.
Boot Options	Set the boot delay when powering on virtual machines or to force BIOS setup and configure failed boot recovery.
Advanced Options	Deactivate acceleration and enable logging, configure debugging and statistics, and change the swap file location. You can also change the latency sensitivity and add configuration parameters.
Fibre Channel NPIV	Control virtual machine access to LUNs on a per-virtual machine basis. N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers.
vApp Options	Enable or deactivate the vApp functionality in a virtual machine. When you enable vApp options, you can view and edit vApp properties, vApp Deployment options, and vApp Authoring options. For example, you can configure an IP allocation policy or a network protocol profile for the vApp. A vApp option that is specified at the level of a virtual machine overrides the settings specified at the level of the vApp.

ThevSphere Client

All administrative functions are available through thevSphere Client .

ThevSphere Client is a cross-platform application that can connect only tovCenter Server. It has a full range of administrative functionality and an extensible plug-in-based architecture. Typical users are virtual infrastructure administrators, help desk, network operations center operators, and virtual machine owners.

Users can use thevSphere Client to accessvCenter Server through a Web browser.vSphere Client uses the VMware API to mediate the communication between the browser and thevCenter Server .

ThevSphere Client introduces some productivity enhancements and usability improvements. Watch the following video to learn about the usability improvements to working with virtual machine hard disks.

Where to Go From Here

You must create, provision, and deploy your virtual machines before you can manage them.

To begin provisioning virtual machines, determine whether to create a single virtual machine and install an operating system and VMware tools, work with templates and clones, or deploy virtual machines, virtual appliances, or vApps stored in Open Virtual Machine Format (OVF).

After you provision and deploy virtual machines into the vSphere infrastructure, you can configure and manage them. You can configure existing virtual machines by modifying or adding hardware or install or upgrade VMware Tools. You might need to manage multitiered applications with VMware vApps or change virtual machine startup and shutdown settings, use virtual machine snapshots, work with virtual disks, or add, remove, or delete virtual machines from the inventory.

Deploying Virtual Machines

VMware supports several methods to provision vSphere virtual machines. What works best in your environment depends on factors such as the size and type of your infrastructure and the goals that you want to achieve.

Create a single virtual machine if no other virtual machines in your environment have the requirements you are looking for, such as a particular operating system or hardware configuration. You can also create a single virtual machine and install an operating system on it, and then use that virtual machine as a template from which to clone other virtual machines. See Create a Virtual Machine with the New Virtual Machine Wizard.

To use a preconfigured virtual machine, deploy and export virtual machines, virtual appliances, and vApps stored in Open Virtual Machine Format (OVF). A virtual appliance is a virtual machine that typically has an operating system and other software installed. You can deploy virtual machines from local file systems and from shared network drives. See Deploying OVF and OVA Templates.

Create a Virtual Machine with the New Virtual Machine Wizard

If no virtual machines in your environment meet your needs, you can create a single virtual machine, for example of a particular operating system or hardware configuration. When you create a virtual machine without a template or clone, you can configure the virtual hardware, including processors, hard disks, and memory. You open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine.

Verify that you have the following privileges:

- **Virtual machine** > **Inventory** > **Create new** on the destination folder or data center.
- **Virtual machine** > **Configuration** > **Add new disk** on the destination folder or data center, if you are adding a new disk.
- **Virtual machine** > **Configuration** > **Add existing disk** on the destination folder or data center, if you are adding an existing disk.

- **Virtual machine** > **Configuration** > **Configure Raw device** on the destination folder or data center, if you are using an RDM or SCSI pass-through device.
- **Virtual machine** > **Configuration** > **Configure Host USB device** on the destination folder or data center, if you are attaching a virtual USB device backed by a host USB device.
- **Virtual machine** > **Configuration** > **Advanced configuration** on the destination folder or data center, if you are configuring advanced virtual machine settings.
- **Virtual machine** > **Configuration** > **Change Swapfile placement** on the destination folder or data center, if you are configuring swap file placement.
- **Virtual machine** > **Configuration** > **Toggle disk change tracking** on the destination folder or data center, if you are enabling change tracking on the virtual machine's disks.
- **Resource** > **Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore** > **Allocate space** on the destination datastore or datastore folder.
- **Network** > **Assign network** on the network that the virtual machine will be assigned to.

To verify the privileges assigned to your role, click **Menu** > **Administration** > **Roles** and select the role.

If you want to create a virtual machine that uses persistent memory, choose a host or a cluster with an available PMem resource.

During the creation process, a default disk is configured for the virtual machine. You can remove this disk and add a new hard disk, select an existing disk, or add an RDM disk on the Virtual Hardware page of the wizard.

1. On the **Select a creation type** page, select **Create a new virtual machine** and click **Next**.
2. On the **Select a name and folder** page, enter a unique name for the virtual machine and select a deployment location.
3. Click **Next**.
4. On the **Select a compute resource** page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

   If creating the virtual machine at the selected location causes compatibility problems, an alarm appears in the **Compatibility** pane.
5. On the **Select storage** page, choose the storage type, the storage policy, and a datastore or datastore cluster where to store the virtual machine files.

Option	Description
Create a virtual machine on a host that has PMem resource	1. Choose the type of storage by selecting the **Standard** or the **PMem** radio button. With the **PMem** storage option, every virtual machine disk file is stored on the host-local PMem datastore by default. You can change the datastore at a later time. The virtual machine home location must be on a non-PMem datastore. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. 2. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 3. To encrypt the virtual machine, select the **Encrypt this virtual machine** check box. 4. Select a datastore or a datastore cluster. 5. If you do not want to use storage DRS with the virtual machine, select the **Disable Storage DRS for this virtual machine** check box.
Create a virtual machine on a host that does not have PMem resource	1. Select a VM storage policy or leave the default one. 2. To encrypt the virtual machine, select the **Encrypt this virtual machine** check box.

Option	Description
	3. Select a datastore or a datastore cluster.

For information about creating an encrypted virtual machine, see *vSphere Security*.

6. On the **Select compatibility** page, select the virtual machine compatibility with ESXi host versions and click **Next**.

   To have access to the latest hardware features, select the latest ESXi host version.

7. On the **Select a guest OS** page, select the guest OS family and version and click **Next**.

   When you select a guest operating system, BIOS or Extensible Firmware Interface (EFI) is selected by default, depending on the firmware supported by the operating system. Mac OS X Server guest operating systems support only EFI. If the operating system supports BIOS and EFI, you can change the default by editing the virtual machine after you create it and before you install the guest operating system. If you select EFI, you cannot boot an operating system that supports only BIOS, and the reverse.

   Important: Do not change the firmware after the guest operating system is installed. The guest operating system installer partitions the disk in a particular format, depending on which firmware the installer was booted from. If you change the firmware, you will not be able to boot the guest.

8. Optional: Enable **Windows Virtualization Based Security**.

   When you enable this option, hardware virtualization, IOMMU, EFI, and secure boot become available to the guest operating system. You must also enable **Virtualization Based Security** within the guest operating system of this virtual machine.

   The **Enable Windows Virtualization Based Security** option is available only for the latest Windows OS versions, for example Windows 10 and Windows Server 2016. For more information about VBS, see the *vSphere Security* documentation.

9. Click **Next**.

10. On the **Customize hardware** page, configure the virtual machine hardware and options and click **Next**.

    You can leave the defaults and configure the virtual machine hardware and options later. For more information, see Configuring Virtual Machine Hardware and Configuring Virtual Machine Options.

    Important: If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

11. On the **Ready to complete** page, review the details and click **Finish**.

The virtual machine appears in the vSphere Client inventory.

Clone a Virtual Machine to a Template

After you create a virtual machine, you can clone it to a template. Templates are primary copies of virtual machines that let you create ready-for-use virtual machines. You can make changes to the template, such as installing additional software in the guest operating system, while preserving the original virtual machine.

If a load generator is running in the virtual machine, stop it before you perform the clone operation.

Verify that you have the following privileges:

- **Virtual machine** > **Provisioning** > **Create template from virtual machine** on the source virtual machine.
- **Virtual machine** > **Inventory** > **Create from existing** on virtual machine folder where the template is created.
- **Resource** > **Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.

- **Datastore** > **Allocate space** on all datastores where the template is created.

You cannot modify templates after you create them. To alter an existing template, you must convert it to a virtual machine, make the required changes, and convert the virtual machine back to a template. To preserve the original state of a template, clone the template to a template.

1. Start the **Clone Virtual Machine To Template** wizard.

Option	Description
From a valid parent object of a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**. 2. On the Select a creation type page, select **Clone virtual machine to template** and click **Next**. 3. On the Select a virtual machine page, select the virtual machine that you want to clone.
From a virtual machine	Right-click the virtual machine and select **Clone** > **Clone to Template**.

2. On the Select a name and folder page, enter a name for the template and select a data center or a folder in which to deploy it.

   The template name determines the name of the files and folder on the disk. For example, if you name the template win8tmp, the template files are named win8tmp.vmdk, win8tmp.nvram, and so on. If you change the template name, the names of the files on the datastore do not change.

   Folders provide a way to store virtual machines and templates for different groups in an organization and you can set permissions on them. If you prefer a flatter hierarchy, you can put all virtual machines and templates in a datacenter and organize them a different way.

3. On the Select a compute resource, select a host or a cluster resource for the template.

   The **Compatibility** pane shows the result from the compatibility checks.

   Important:

   If the virtual machine that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

   If the virtual machine that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the template will use the storage policy and datastore selected for the configuration files of the source virtual machine.

4. On the Select storage page, select the datastore or datastore cluster in which to store the template configuration files and all of the virtual disks. Click **Next**.

Option	Description
Clone a virtual machine that has vPMem hard disks	1. Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks are stored on a standard datastore. If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine. If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

Option	Description
	For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. 2. From the **Select virtual disk format** drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine. 3. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 4. Select a datastore or a datastore cluster. 5. Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine. 6. Turn on the **Configure per disk** option to select a separate datastore or a datastor cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.
Clone a virtual machine that does not have vPMem hard disks	1. Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. The **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine. **Thick Provision Eager Zeroed** is a type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat file format (`-flat.vmdk`), the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks. The **Thin Provision** format saves storage space. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it. 2. Select a VM storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.

Important: You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

5. On the Ready to complete page, review the template settings and click **Finish**.

   The progress of the clone task appears in the **Recent Tasks** pane. When the task completes, the template appears in the inventory.

Deploy a Virtual Machine from a Template

Deploying a virtual machine from a template creates a virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties that are configured for the template.

You must have the following privileges to deploy a virtual machine from a template:

- **Virtual machine** > **Inventory** > **Create from existing** on the data center or virtual machine folder.
- **Virtual machine** > **Configuration** > **Add new disk** on the data center or virtual machine folder. Required only if you customize the original hardware by adding a new virtual disk.
- **Virtual machine** > **Provisioning** > **Deploy template** on the source template.
- **Resource** > **Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore** > **Allocate space** on the destination datastore.
- **Network** > **Assign network** on the network to which the virtual machine is assigned. Required only if you customize the original hardware by adding a new network card.
- **Virtual machine** > **Provisioning** > **Customize** on the template or template folder if you are customizing the guest operating system.
- **Virtual machine** > **Provisioning** > **Read customization specifications** on the root vCenter Server if you are customizing the guest operating system.
- **Virtual machine** > **Inventory** > **Create new** on the destination folder or data center.
- **vApp** > **Import**

1. Start the **Deploy From Template** wizard.

Option	Description
From a valid parent object of a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**. 2. On the Select a creation type page, select **Deploy from template** and click **Next**. 3. On the Select a template page, select the template that you want to use.
From a template	Right-click a template and select **New VM from This Template**.

2. On the **Select a name and folder** page, enter a unique name for the virtual machine and select a deployment location.
3. On the **Select a compute resource** page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

   The virtual machine will have access to the resources of the selected object.

   Important:

   If the template that you deploy has an has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

   If the template that you deploy does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

   If creating the virtual machine at the selected location causes compatibility problems, an alarm appears in the **Compatibility** pane.

4. On the **Select storage** page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

Option	Description
Deploy a virtual machine from a template that has vPMem hard disks	1. Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks will be stored on a standard datastore. If you select the **PMem** mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine. If you select the **Hybrid** mode, all PMem virtual disks will remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. 2. From the **Select virtual disk format** drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine. 3. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 4. Select a datastore or a datastore cluster. 5. Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine. 6. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.
Deploy a virtual machine from a template that does not have vPMem hard disks	1. Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. The **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine. **Thick Provision Eager Zeroed** is a type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types o disks. The **Thin Provision** format saves storage space. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it. 2. Select a VM storage policy or leave the default one.

Option	Description
	3. Select a datastore or a datastore cluster. 4. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.

5. On the **Select clone options** page, select additional customization options for the new virtual machine.

   You can choose to customize the guest operating system or the virtual machine hardware. You can also choose to power on the virtual machine after its creation.

6. Optional: On the **Customize guest OS** page, apply a customization specification to the virtual machine.

   Customizing the guest OS prevents from conflicts that might occur if you deploy virtual machines with identical settings, such as duplicate computer names.

   Note: To access customization options for Windows guest operating systems, Microsoft Sysprep tools must be installed on the vCenter Server system. The Sysprep Tool is built into the Windows Vista and Windows 2008 and later operating systems. For details about this and other customization requirements, see Guest Operating System Customization Requirements.

Option	Description
Select an existing specification	Select a customization specification from the list.
Create a specification	Click the **Create a new specification** icon, and complete the steps in the wizard.
Create a specification from an existing specification	1. Select a customization specification from the list. 2. Click the **Create a spec from an existing spec** icon, and complete the steps in the wizard.

7. Optional: On the **Customize hardware** page, configure the virtual machine hardware and options and click **Next**.

   You can leave the defaults and configure the virtual machine hardware and options later. For more information, see Configuring Virtual Machine Hardware and Configuring Virtual Machine Options.

   Important: If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

8. On the Ready to complete page, review the information and click **Finish**.

Clone an Existing Virtual Machine

Cloning a virtual machine creates a virtual machine that is a copy of the original. The new virtual machine is configured with the same virtual hardware, installed software, and other properties that were configured for the original virtual machine.

If a load generator is running in the virtual machine, before you perform the clone operation, you must stop the load generator.

You must have the following privileges to clone a virtual machine:

- **Virtual machine** > **Provisioning** > **Clone virtual machine** on the virtual machine you are cloning.
- **Virtual machine** > **Inventory** > **Create from existing** on the datacenter or virtual machine folder.
- **Virtual machine** > **Configuration** > **Add new disk** on the datacenter or virtual machine folder.

- **Resource** > **Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore** > **Allocate space** on the destination datastore or datastore folder.
- **Network** > **Assign network** on the network to which you assign the virtual machine.
- **Virtual machine** > **Provisioning** > **Customize** on the virtual machine or virtual machine folder if you are customizing the guest operating system.
- **Virtual machine** > **Provisioning** > **Read customization specifications** on the root vCenter Server if you are customizing the guest operating system.
- If the virtual machine that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have an available PMem resource. Otherwise, you cannot proceed with the task
- If the virtual machine that you clone does not have an NVDIMM device, but has virtual PMem hard disks, the destination host or cluster must have an available PMem resource. Otherwise, all hard disks of the destination virtual machine will use the storage policy and datastore selected for the configuration files of the source virtual machine.
- To access customization options for Windows guest operating systems, Microsoft Sysprep tools must be installed on the vCenter Server system. Sysprep Tool is built into the Windows Vista and Windows 2008 and later operating systems. For details about this and other customization requirements, see Guest Operating System Customization Requirements.

For information about persistent memory and PMem storage, see the *vSphere Resource Management* guide.

For information how to configure the virtual machine hardware options, see Configuring Virtual Machine Hardware and Configuring Virtual Machine Options

Note: When heavily loaded applications, such as load generators, are running in the guest operating system during a clone operation, the virtual machine quiesce operation might fail. VMware Tools might be denied CPU resources and time out. You can quiesce the virtual machines running lower I/O disk operation.

Important: If you clone an encrypted virtual machine, you cannot change the storage policy. For information about cloning an encrypted virtual machine, see *vSphere Security*.

1. Start the **Clone Existing Virtual Machine** wizard.

Option	Action
From a valid parent object of a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, cluster, vApp, resource pool, or host, and select **New Virtual Machine**. 2. On the **Select a creation type** page, select **Clone an existing virtual machine**, and click **Next**. 3. On the **Select a virtual machine** page, select the virtual machine that you want to clone.
From a virtual machine	Right-click a virtual machine and select **Clone** > **Clone to Virtual Machine**.

2. On the **Select a name and folder** page, enter a unique name for the new virtual machine, select a deployment location, and click **Next**.

   The template name determines the name of the files and folder on the disk. For example, if you name the template `win8tmp`, the template files are named `win8tmp.vmdk`, `win8tmp.nvram`, and so on. If you change the template name later, the names of the files on the datastore do not change.

   Folders provide a way to store virtual machines and templates for different groups in an organization and you can set permissions on them. If you prefer a flatter hierarchy, you can put all virtual machines and templates in a data center and organize them in a different way.

3. On the **Select a compute resource** page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

   The **Compatibility** pane shows the result from the compatibility checks.

4. On the **Select storage** page, select the datastore or datastore cluster in which to store the template configuration files and all virtual disks.

Option	Action
Clone a virtual machine that has vPMem hard disks	1. Select the type of storage for the template by clicking the **Standard**, the **PMem**, or the **Hybrid** radio button. – If you select the **Standard** mode, all virtual disks are stored on a standard datastore. – If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine. – If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Your choice of a VM storage policy and datastore or datastore cluster affects the non-PMem disks. 2. From the **Select virtual disk format** drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine. 3. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 4. Select a datastore or a datastore cluster. 5. Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine. 6. Enable the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.
Clone a virtual machine that does not have vPMem hard disks	1. Select the disk format for the virtual machine virtual disks. – The **Same format as source** option uses the same disk format as the source virtual machine. – The **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. The space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine. – **Thick Provision Eager Zeroed** is a type of thick virtual disk that supports clustering features such as Fault tolerance. The space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks. – The **Thin Provision** format saves storage space. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it. 2. Select a VM storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Enable the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.

5. Click **Next**.
6. On the **Select clone options** page, select additional customization options for the new virtual machine and click **Next**.

   You can choose to customize the guest operating system or the virtual machine hardware. You can also choose to power on the virtual machine after its creation.

7. Optional: On the **Customize guest OS** page, apply a customization specification to the virtual machine and click **Next**.

   Customizing the guest operating system prevents from conflicts that might occur if you or other users clone virtual machines with identical settings, such as duplicate computer names.

Option	Action
Select an existing specification	Select a customization specification from the list.
Override	To change the guest customization specification for this deployment only, click **Override**, complete the steps in the **Override VM Customization Specification** wizard, and click **OK**.

8. Optional: On the **User settings** page, specify the required settings for the virtual machine.

   This page of the wizard appears only if the selected specification requires additional customization.

9. Optional: On the **Customize hardware** page, configure the virtual machine hardware and options and click **Next**.

   You can leave the defaults and configure the virtual machine hardware and options later.

   Important: If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. You must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

10. On the **Ready to complete** page, review the virtual machine settings and click **Finish**.

The new virtual machine appears in the inventory.

Cloning a Virtual Machine with Instant Clone

You can use the Instant Clone technology to create powered on virtual machines from the running state of another powered on virtual machine. The result of an Instant Clone operation is a new virtual machine that is identical to the source virtual machine. With Instant Clone you can create new virtual machines from a controlled point in time. Instant cloning is very convenient for large scale application deployments because it ensures memory efficiency and allows for creating numerous virtual machines on a single host.

The result of an Instant Clone operation is a virtual machine that is called a destination virtual machine. The processor state, virtual device state, memory state, and disk state of the destination virtual machine are identical to those of the source virtual machine. To avoid network conflicts, you can customize the virtual hardware of the destination virtual machine during an Instant Clone operation. For example, you can customize the MAC addresses of the virtual NICs or the serial port configurations of the destination virtual machine. vSphere 6.7 and later does not support customization of the guest OS of the destination virtual machine. For information about manual guest OS customization, see the *vSphere Web Services SDK Programming Guide*.

During an Instant Clone operation, the source virtual machine is stunned for a short period of time, less than 1 second. While the source virtual machine is stunned, a new writable delta disk is generated for each virtual disk and a checkpoint is taken and transferred to the destination virtual machine. The destination virtual machine then powers on by using the source's checkpoint. After the destination virtual machine is fully powered on, the source virtual machine also resumes running.

Instant Cloned virtual machines are fully independent vCenter Server inventory objects. You can manage Instant Cloned virtual machines like regular virtual machines without any restrictions.

Starting with vSphere 6.7, you can Instant Clone a virtual machine only through the API calls.

For information about Instant Clone, see the *vSphere Web Services SDK Programming Guide*.

Clone a Template to a Template

After you create a template, you can clone it to a template. Templates are primary copies of virtual machines that let you create ready-for-use virtual machines. You can change the template, for example, installing additional software in the guest operating system, while preserving the state of the primary template.

Verify that you have the following privileges:

- **Virtual machine** > **Provisioning** > **Clone template** on the source template.
- **Virtual machine** > **Inventory** > **Create from existing** on the folder where the template is created.
- **Datastore** > **Allocate space** on all datastores where the template is created.

1. Start the **Clone Template to Template** wizard.

Option	Description
From a valid parent object of a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine and select **New Virtual Machine**. 2. Select **Clone template to template** and click **Next**. 3. On the **Select a template to clone** page, browse to the template that you want to clone or accept the default one.
From a template	Right-click a template and select **Clone to Template**.

2. On the **Select a name and folder** page, enter a unique name for the template and select the data center or folder in which to deploy it.

   The template name determines the name of the files and folder on the disk. For example, if you name the template win10tmp, the template files are named win10tmp.vmdk, win10tmp.nvram, and so on. If you change the template name, the names of the files on the datastore do not change.

   Folders provide a way to store virtual machines and templates for different groups in an organization and you can set permissions on them. If you prefer a flatter hierarchy, you can put all virtual machines and templates in a data center and organize them in a different way.

3. Click **Next**.
4. On the **Select a compute resource** page, select a host or cluster resource for the template.

   The **Compatibility** pane shows the result from the compatibility checks.

   Important:

   If the template that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

   If the template that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the template use the storage policy and datastore selected for the configuration files of the source template.

5. On the **Select storage** page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks.

Option	Description
Clone a virtual machine that has vPMem hard disks	1. Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks are stored on a standard datastore. If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.

Option	Description
	If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. 2. From the **Select virtual disk format** drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine. 3. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 4. Select a datastore or a datastore cluster. 5. Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine. 6. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance issues. You can also convert a standard hard disk to a PMem hard disk.
Clone a virtual machine that does not have vPMem hard disks	1. Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. The **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine. **Thick Provision Eager Zeroed** is a type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types o disks. The **Thin Provision** format saves storage space. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to its maximum capacity allocated to it. 2. Select a VM storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance issues. You can also convert a standard hard disk to a PMem hard disk.

Important: If you clone an encrypted virtual machine, you cannot change the storage policy. For information about cloning an encrypted virtual machine, see *vSphere Security*.

6. Click **Next**.
7. On the **Ready to complete** page, review the template settings and click **Finish**.

The progress of the clone task appears in the **Recent Tasks** pane. When the task completes, the template appears in the inventory.

Convert a Template to a Virtual Machine

Converting a template to a virtual machine changes the template. This action does not make a copy. You convert a template to a virtual machine to edit the template. You might also convert a template to a virtual machine if you do not need to preserve it as a golden image for deploying virtual machines.

Verity that you have the following privileges:

- **Virtual machine** > **Provisioning** > **Mark as virtual machine** on the source template.
- **Resource** > **Assign virtual machine to resource pool** on the resource pool where the virtual machine runs.

1. Start the **Convert Template to Virtual Machine** wizard.

Option	Description
From a valid parent object of a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine and select **New Virtual Machine**. 2. On the **Select a creation type** page, select **Convert template to virtual machine**, and click **Next**. 3. On the **Select a template** page of the wizard, select a template to deploy from the list.
From a template	Right-click the template and select **Convert to Virtual Machine**.

2. On the **Select a compute resource** page, select the host, cluster, vApp, or resource pool for the virtual machine to run in.

   Important:

   If the template that you convert has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

   If the template that you convert does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine use the storage policy and datastore selected for the configuration files of the source template.

   The **Compatibility** pane shows the result from the compatibility checks.
3. Click **Next**.
4. On the **Ready to complete** page, review the settings, and click **Finish**.

The virtual machine appears in the inventory.

Deploying OVF and OVA Templates

You can export virtual machines, virtual appliances, and vApps in Open Virtual Format (OVF) and Open Virtual Appliance (OVA) . You can then deploy the OVF or OVA template in the same environment or in a different environment.

Note: In vSphere 6.5 and later, you cannot export OVA templates, OVF templates is the only option.

OVF and OVA File Formats and Templates

OVF is an open standard which contains multiple files as a package. For example, `.ovf`, `.vmdk`, `.nvram`, and so on. OVF supports exchange of virtual appliances across products and platforms. OVA is a single file distribution of the OVF

file package. When you export a virtual machine as an OVF file, you create a directory that contains an OVF file and the virtual disk files.

The OVF and OVA formats offer the following advantages:

- OVF and OVA files are compressed, allowing for faster downloads.
- The vSphere Web Client validates an OVF or OVA file before importing it, and ensures that it is compatible with the intended destination server. If the appliance is incompatible with the selected host, it cannot be imported and an error message appears.
- OVF and OVA can encapsulate multi-tiered applications and more than one virtual machine.

Exporting OVF templates allows you to create virtual appliances that other users can import later. You can use the export function to distribute pre-installed software as a virtual appliance, or to distribute template virtual machines to users. You can make the OVF or OVA file available to users who cannot access your vCenter Server inventory.

Deploying an OVF or OVA template allows you to add pre-configured virtual machines or vApps to your vCenter Server or ESXi inventory. Deploying an OVF or OVA template is similar to deploying a virtual machine from a template. However, you can deploy an OVF or OVA template from any local file system accessible from the vSphere Web Client, or from a remote Web server. The local file systems can include local disks (such as `C:`), removable media (such as CDs or USB keychain drives), and shared network drives.

Deploy an OVF or OVA Template

You can deploy an OVF or OVA template from a local file system or from a URL.

Some of the pages in the **Deploy OVF Template** wizard only appear if the OVF template that you deploy requires additional customization, contains deployment options or has one or multiple vService dependencies.

1. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **Deploy OVF Template**.

   The **Deploy OVF Template** wizard opens.

2. On the **Select an OVF template** page, specify the location of the source OVF or OVA template and click **Next**.

Option	Action
URL	Type a URL to an OVF or OVA template located on the Internet. Supported URL sources are HTTP and HTTPS. **Note:** Verify that all files from the OVF package are at the same location of the OVF descriptor file. Example: `http://vmware.com/VMTN/appliance.ovf`.
Local file	Click **Browse** and select all the files associated with an OVF template or OVA file. This includes files such as `.ovf`, `.vmdk`, etc. If you do not select all the required files, a warning message displays.

3. On the **Select a name and folder** page, enter a unique name for the virtual machine or vApp, select a deployment location, and click **Next**.

   The default name for the virtual machine is the same as the name of the selected OVF or OVA template. If you change the default name, choose a name that is unique within each vCenter Server virtual machine folder.

   The default deployment location for the virtual machine is the inventory object where you started the wizard.

4. On the **Select a compute resource** page, select a resource where to run the deployed VM template, and click **Next**.

5. On the **Review details** page, verify the OVF or OVA template details and click **Next**.

Option	Description
Publisher	Publisher of the OVF or OVA template, if a certificate included in the OVF or OVA template file specifies a publisher.

Option	Description
Download size	Size of the OVF or OVA file.
Size on disk	Size on disk after you deploy the OVF or OVA template.

6. Optional: On the **Configuration** page, select a deployment configuration and click **Next**.
7. On the **Select storage** page, define where and how to store the files for the deployed OVF or OVA template.
   a) Select the disk format for the virtual machine virtual disks.

Format	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine.
Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat file format (`-flat.vmdk`), the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk requires based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

   b) Select a VM Storage Policy.

      This option is available only if storage policies are enabled on the destination resource.
   c) Optional: Enable the **Show datastores from Storage DRS clusters** check box to choose individual datastores from Storage DRS clusters for the initial placement of the virtual machine.
   d) Select a datastore to store the deployed OVF or OVA template.

      The configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.

   Note: If you want to use the API calls to deploy an OVF template that contains vPMem hard disks and that has been exported from a content library, consult https://kb.vmware.com/kb/52370.
8. On the **Select networks** page, select a source network and map it to a destination network. Click **Next**.

   The Source Network column lists all networks that are defined in the OVF or OVA template.
9. Optional: On the **Customize template** page, customize the deployment properties of the OVF template and click **Next**.
10. Optional: On the **vService bindings** page, select a binding service provider and click **Next**.
11. On the **Ready to complete** page, review the page and click **Finish**.

A new task for creating the virtual machine appears in the Recent Tasks pane. After the task is complete, the new virtual machine is created on the selected resource.

Export an OVF Template

An OVF template captures the state of a virtual machine or vApp into a self-contained package. The disk files are stored in a compressed, sparse format.

Power off the virtual machine or vApp.

Required privilege: **vApp** > **Export**

1. Navigate to a virtual machine or vApp and from the **Actions** menu, select **Template** > **Export OVF Template**.
2. In the **Name** field, enter the name of the template.
   For example, enter `MyVm`.

   Note: When you export an OVF template with a name that contains asterisk (*) characters, those characters turn into underscore (_) characters.
3. Optional: In the **Annotation** field, enter a description.
4. Select the **Enable advanced options** check box if you want to include additional information or configurations in the exported template.

   The advanced settings include information about the BIOS UUID, MAC addresses, boot order, PCI Slot numbers, and configuration settings used by other applications. These options limit portability.
5. To save each file associated with the template (`.ovf`, `.vmdk`, `.mf`), click **OK** and respond to the prompts .

Browse VMware Virtual Appliance Marketplace

The Virtual Appliance Marketplace contains a variety of virtual appliances packaged in OVF format that you can download and deploy in your vSphere environment.

1. Go to the Virtual Appliance Marketplace, which is part of the VMware Solution Exchange.
2. Search the Marketplace to find a prepackaged application.
3. Log in and download the appliance.
4. Deploy the appliance in your vSphere environment.

Using Content Libraries

Content libraries are container objects for VM and vApp templates and other types of files, such as ISO images, text files, and so on. To deploy virtual machines and vApps in the vSphere inventory, you can use the templates in the library. You can also use content libraries to share content across vCenter Server instances in the same or different locations. Sharing templates and files results in consistency, compliance, efficiency, and automation in deploying workloads at scale.

A content library stores and manages content in the form of library items. A single library item can consist of one file or multiple files. For example, the OVF template is a set of files (`.ovf`, `.vmdk`, and `.mf`). When you upload an OVF template to the library, you upload the entire set of files, but the result is a single library item of the OVF Template type.

Starting with vSphere 7.0 Update 3, you can protect the OVF items by applying default OVF security policy to a content library. The OVF security policy enforces strict validation on OVF items when you deploy or update the item, import items, or synchronize OVF and OVA templates. To make sure that the OVF and OVA templates are signed by a trusted certificate, you can add the OVF signing certificate from a trusted CA.

In previous versions of vSphere, content libraries supported only OVF templates. As a result, VM and vApp templates were both converted to OVF files when you uploaded them to a content library. Starting with vSphere 6.7 Update 1, content libraries also support VM templates. So, templates in the content library can either be of the OVF Template type, or the VM Template type. vApp templates are still converted to OVF files when you upload them to a content library.

You create and manage a content library from a single vCenter Server instance, but you can distribute the content to other vCenter Server instances if HTTP(S) traffic is allowed between the two systems. The distribution of VM templates additionally requires that the respective vCenter Server instances are in Enhanced Linked Mode or Hybrid Linked Mode and that the respective hosts are connected through a network.

You can create two types of content libraries.

- You can create a local content library to store and manage content in a single vCenter Server instance. If you want to share the contents of that library, you can enable publishing. When you enable publishing, other users can subscribe to the library and use its content. Alternatively, you can create subscriptions for the library, which gives you control over the distribution of content.
- You can create a subscribed content library to subscribe to a published library and use its contents. You cannot upload or import items into a subscribed library. Subscribers only use the content in the published library, but it is the administrator of the published library who manages the templates.

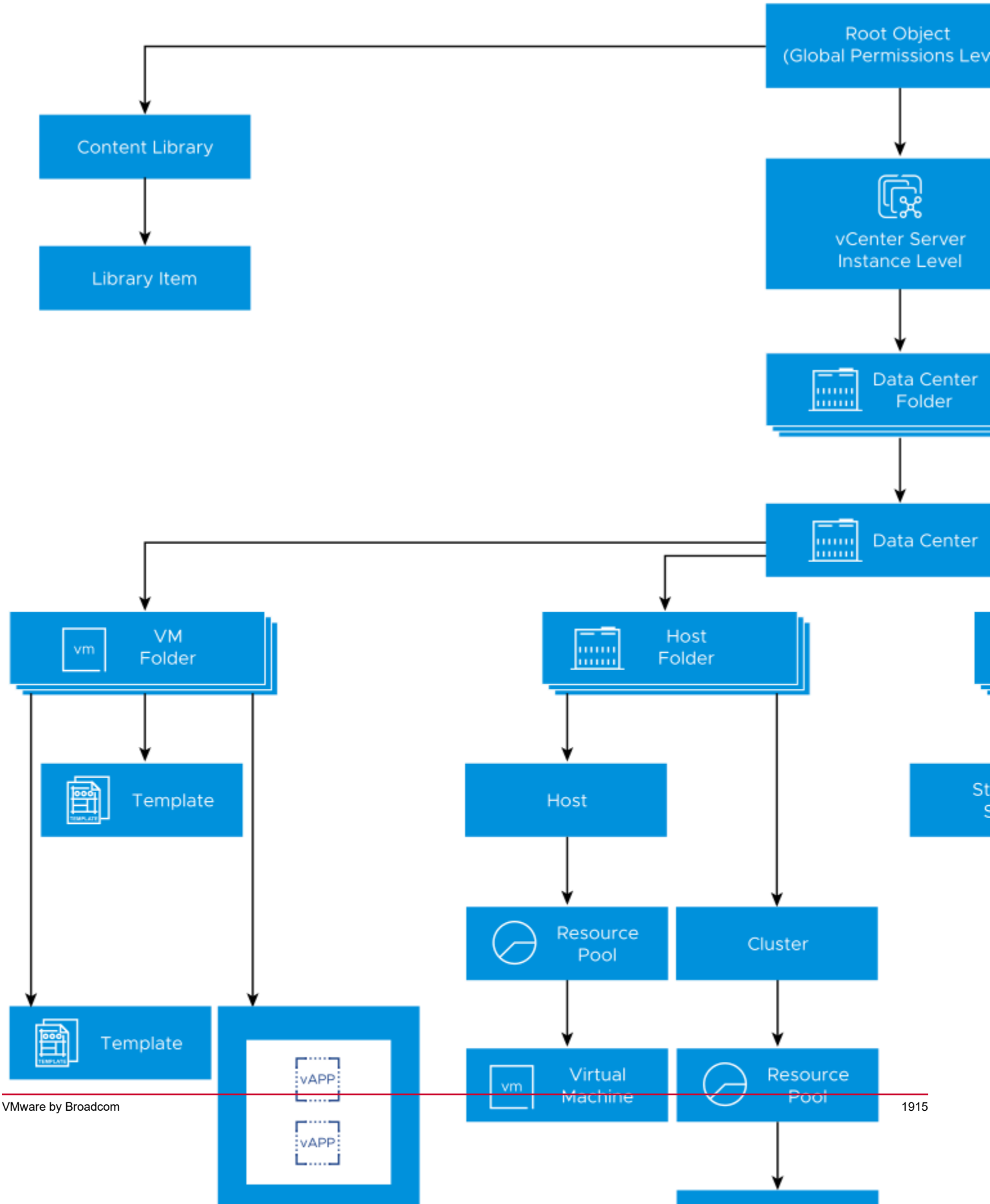
Hierarchical Inheritance of Permissions for Content Libraries

vSphere objects inherit permissions from a parent object in the hierarchy. Content libraries work in the context of a single vCenter Server instance. However, content libraries are not direct children of a vCenter Server system from an inventory perspective.

The direct parent for content libraries is the global root. This means that if you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and so on, but does not apply to the content libraries that you see and operate with in this vCenter Server instance. To assign a permission on a content library, an Administrator must grant the permission to the user as a global permission. Global permissions support assigning privileges across solutions from a global root object.

The figure illustrates the inventory hierarchy and the paths by which permissions can propagate.

Figure 48: vSphere Inventory Hierarchy



To let a user manage a content library and its items, an Administrator can assign the Content Library Administrator role to that user as a global permission. The Content Library Administrator role is a sample role in the vSphere Client.

Users who are Administrators can also manage libraries and their contents. If a user is an Administrator at a vCenter Server level, they have sufficient privileges to manage the libraries that belong to this vCenter Server instance, but cannot see the libraries unless they have a Read-Only role as a global permission.

For example, a user has an Administrator role that is defined at a vCenter Server level. When the Administrator navigates to Content Libraries in the object navigator, he sees 0 libraries despite there are existing libraries in the vSphere inventory of that vCenter Server instance. To see the libraries, the Administrator needs a Read-Only role assigned as a global permission.

Administrators whose role is defined as a global permission can see and manage the libraries in all vCenter Server instances that belong to the global root.

Because content libraries and their children items inherit permissions only from the global root object, when you navigate to a library or a library item and click **Configure** tab, you can see there is no **Permissions** tab. An Administrator cannot assign individual permissions on different libraries or different items within a library.

Content Library Administrator Role

vCenter Server provides a sample role that allows you to give users or groups privileges to manage content libraries.

Content Library Administrator role is a predefined role that gives a user privileges to monitor and manage a library and its contents.

If a user has this role on a library, that user can perform the following tasks on that library.

- Create, edit, and delete local or subscribed libraries.
- Create and delete subscriptions to a local library with publishing enabled.
- Publish a library or a library item to a subscription.
- Synchronize a subscribed library and synchronize items in a subscribed library.
- View the item types supported by the library.
- Configure the global settings for the library.
- Import items to a library.
- Export library items.

Create a Library

In the vSphere Client, you can create a local or a subscribed content library. By using content libraries, you can store and manage content in one vCenter Server instance. Alternatively, you can distribute content across vCenter Server instances to increase consistency and facilitate the deployment workloads at scale.

Required privileges:

- **Content library** > **Create local library** or **Content library** > **Create subscribed library** on the vCenter Server instance where you want to create the library.
- **Datastore** > **Allocate space** on the destination datastore.

You can create a local content library and populate it with templates and other types of files. You can then use the content library templates to deploy virtual machines or vApps in your virtual environment. You can also share the contents of your local library with users from other vCenter Server instances.

Note: VM Templates cannot be stored in a library that uses NFS or SMB storage. OVF templates can only be stored on the datastore that is associated with the content library.

You can also create a subscribed library to use at will the contents of an already existing published local library.

By using the OVF security policy, you can protect the items of your content library.

1. Navigate to **Menu** > **Content Libraries**.
2. Click **Create**.
   The **New Content Library** wizard opens.
3. On the **Name and location** page, enter a name, select a vCenter Server instance for the content library and click **Next**.
4. On the **Configure content library** page, select the type of content library that you want to create.

Option	Description
Local content library	A local content library is accessible only in the vCenter Server instance where you create it by default. 1. To make the content of the library available to other vCenter Server instances, select **Enable publishing** . 2. If you want to require a password for accessing the content library, select **Enable authentication** and set a password. 3. Click **Next**.
Subscribed content library	A subscribed content library originates from a published content library. Use this option to take advantage of already existing content libraries. **Note:** If the published content library does not have a security policy enabled, you cannot apply the OVF default security policy to the subscribed content library. If you create a subscribed library, depending on the **Subscription URL** that you provide, the system performs a check to determine whether the provided URL can have a security policy enabled or not. To see up-to-date content, you can synchronize the subscribed library with the published library, but you cannot add or remove content from the subscribed library. Only an administrator of the published library can add, modify, and remove contents from the published library. To subscribe to a library, provide the following information: 1. In the **Subscription URL** text box, enter the URL address of the published library. **Note:** The system performs a check to determine whether the **Subscription URL** that you provide can have a security policy enabled or not. 2. If authentication is enabled on the published library, select **Enable authentication** and enter the publisher password. 3. Select a download method for the contents of the subscribed library. – To download a local copy of all the items in the published library immediately after subscribing to it, select **immediately**. – To save storage space, select **when needed**. You download only the metadata for the items in the published library. If you must use an item, synchronize the item or the entire library to download its content.

Option	Description
	4. If prompted, accept the SSL certificate thumbprint. The SSL certificate thumbprint is stored on your system until you delete the subscribed content library from the inventory. 5. Click **Next**.

5. Optional: On the **Apply security policy** page, select **Apply Security Policy** and select **OVF default policy**.
6. Click **Next**.
7. On the **Add storage** page, select datastore as a storage location for the content library contents and click **Next**.
8. On the **Ready to complete** page, review the details and click **Finish**.

Edit a Content Library

In the vSphere Client, you can edit a local library by changing its name, description, or tags. You can also change the configuration settings of a local or subscribed content library.

The privileges that you need depend on the task that you want to perform.

Task	Privilege
Edit Local Content Library Settings	**Content library** > **Update library** and**Content library** > **Update local library** on the library.
Edit Subscribed Content Library Settings	**Content library** > **Update subscribed library** and**Content library** > **Probe subscription information** on the subscribed library.
Delete Content Library	**Content library** > **Delete subscribed library** or**Content library** > **Delete local library** depending on the type of library that you want to delete.

To share the contents of a local library across multiple vCenter Server instances, you must enable publishing for the library. From the **Edit Setting** dialog box, you can obtain the URL of your library and send it to other users to subscribe.

If a library is already published, you can change its password for authentication. To keep access to the published library, users who are subscribed to your library must update the password.

For subscribed libraries, you can change the download method or enable automatic synchronization with the published library.

1. Navigate to **Menu** > **Content Libraries**.
2. Right-click a content library and select the action that you want to perform.
   - To edit the content library description, select **Edit notes**.
   - To change the name of the content library, select **Rename**.
   - To assign a tag to the content library, select **Tags** > **Assign Tag**.
   - To remove a tag from the content library, select **Tags** > **Remove Tag**.

     For information about tags and tag categories, see the *vCenter Server and Host Management* documentation.
   - To delete the content library, select **Delete**.

3. To edit the configuration settings of a content library, right-click the content library and click **Edit Settings**.
   The changes that you can make depend on the type of content library that you edit.

Content Library Type	Action
Local content library that is unpublished	To share the contents of a local library with other users, you can enable the publishing of the local library. 1. To publish the local library and share its contents with other users, select the **Enable publishing** check box. 2. To obtain the URL of your library and distribute it, click the **Copy Link** button. 3. Select **Enable user authentication for access to this content library** and set a password for the library. If you protect the library with a password, you must provide both the URL and the password to users who want to subscribe to your library. 4. To activate or deactivate the security policy, select or deselect the **Apply Security Policy**. When you deactivate the security policy of a content library, you cannot reuse the existing OVF items. 5. Click **OK**.
Local content library that is published	You can change the following settings of a local library that is published. • You can copy the subscription URL to your library and send it to other users to subscribe. • You can unpublish the library by deselecting the **Enable publishing** check box. Users who are currently subscribed to this library can no longer synchronize to the library, but they can still use the previously synchronized content. • You can activate or deactivate authentication for the library. • In the vSphere Client, you can change the password for authentication if the library is published and password-protected. a. Enter the current password and the new password. Confirm the new password. b. Click **OK**. • To activate or deactivate the security policy, select or deselect the **Apply Security Policy**. When you deactivate the security policy of a content library, you cannot reuse the existing OVF items.
Subscribed content library	You can change the following settings of a subscribed library: • Activate or deactivate the automatic synchronization with the published library. • Update the password for authentication to the published library. • Select a download method. You can either download all library content immediately or download the library content only when needed. If you switch from the option to download content only when needed to the option to download all library content immediately, a synchronization task starts and content starts downloading. The number and size of items in the published library determine the amount of time and network bandwidth that the task requires. • To activate or deactivate the security policy, select or deselect the **Apply Security Policy**. When you deactivate the security policy of a content library, you cannot reuse the existing OVF items.

Configure Advanced Content Library Settings

You can monitor and configure the content library service settings across different vCenter Server instances. This advanced configuration ensures the consistency in your environment.

Verify that you are a member of the **SystemConfiguration.Administrators** group in the vCenter Single Sign-On domain.

1. Navigate to **Menu** > **Content Libraries**.
2. From the **Content Libraries** pane, select a library and click **Advanced**.
   The **Advanced Configuration** dialog box opens.
3. Configure the parameters.

Configuration Parameter	Description
Library Auto Sync Enabled	Enables automatic synchronization of subscribed content libraries.
Library Auto Sync Refresh Interval (minutes)	Interval between two consequent automatic synchronizations of the subscribed content library. Measured in minutes.
Library Auto Sync Setting Refresh Interval (seconds)	Interval after which the refresh interval for the automatic synchronization settings of the subscribed library will be updated if it has been changed. Measured in seconds. If you change the refresh interval, you must restart the vCenter Server system.
Library Auto Sync Start Hour	The time of the day when the automatic synchronization of a subscribed content library starts.
Library Auto Sync Stop Hour	The time of the day when the automatic synchronization of a subscribed content library stops. Automatic synchronization stops until the start hour.
Library Maximum Concurrent Sync Items	Maximum number of concurrently synchronizing library items for each subscribed library.
Max concurrent NFC transfers per ESX host	Maximum concurrent NFC transfers limit per ESXi host.
Maximum Bandwidth Consumption	Bandwidth usage threshold across all transfers, measured in Mbps where 0 means unlimited bandwidth.
Maximum Number of Concurrent Priority Transfers	Concurrent transfer limit for priority files. If exceeded, transfers are queued. This threadpool is used only to transfer priority objects. For example, OVF. If you change the concurrent transfer limit for priority files, you must restart the vCenter Server system.
Maximum Number of Concurrent Transfers	Concurrent transfer limit. If exceeded, transfers are queued. If you change the concurrent transfer limit, you must restart the vCenter Server system.

4. Click **Save**.
5. From the **vCenter Server** drop-down menu, select the vCneter Server instance whose settings you want to configure.

   Note: The **vCenter Server** drop-down menu appears only if your environment has more than one vCenter Server instance.
6. Edit the configuration parameters and click **Save**.
7. To apply the changes that require a content library service restart, click **Restart from VAMI**.
   The vCenter Server Management Interface opens and you can log in to it with your credentials.

Managing a Publisher Local Library

To share the contents of a local library with users from other vCenter Server instances, activate publishing for the library. If publishing is activated, other users can subscribe to the published library and use its contents. As an administrator, you can also create subscriptions for the library to gain control over the distribution of content.

A publisher library is a local library with subscriptions.

Note: You cannot create subscriptions to a local library that does not have publishing activated. You also cannot deactivate publishing for a library that already has subscriptions. To deactivate publishing for a local library, you must first delete all of its subscriptions.

To avoid name collisions and failures when you publish content from the publisher library, the publisher and subscriber libraries must have unique folders dedicated to them.

Local Libraries

You use a local library to store and manage items in a single vCenter Server instance. When you activate publishing for the library, users from other vCenter Server instances can subscribe to it and gain access to the library items. In this case, only the subscriber initiates and controls the synchronization of content between the published library and the subscribed library.

If publishing is activated, you can also create subscriptions to the local library. Creating a subscription creates a new subscribed library or links the publisher library to an existing subscriber. Unlike regular subscribed libraries, subscriptions give the administrator of the local library control over the distribution of content library items.

Using Subscriptions

When you create a subscription for a local library, the result is a subscribed library. A publisher library is aware of its subscriptions. Subscriptions activate the administrator of the publisher library to control the content distribution. With subscriptions, content is distributed either when the subscriber initiates synchronization, or when the administrator of the local library publishes the library items to one or more of the existing subscriptions.

When you use subscriptions, you have the flexibility to decide how much of the library content you want to share with the subscribers. For example, you can publish some or all library items. You can also publish content to selected subscribers or to all subscribers.

The use of subscriptions allows content distribution between a publisher and a subscriber in the following scenarios.

- The publisher and subscriber are in the same vCenter Server instance.
- The publisher and subscriber are in vCenter Server instances that are in Enhanced Linked Mode.
- The publisher and subscriber are in vCenter Server instances that are in Hybrid Linked Mode. For more information about Hybrid Linked Mode, see the documentation.

  Note: Publishing content is possible only from an on-premises publisher to a cloud subscriber, and not in the reverse scenario.

Limitations in Content Distribution

Content is distributed when a publisher library publishes content to its subscribers or when a subscriber synchronizes the content in the respective subscribed library with the published library. You can publish and synchronize a single content library item or an entire library. The following limitations exist in the distribution of content between a published and a subscribed library.

- You can publish only VM templates. If you publish an entire library that contains both VM templates and OVF templates, only the VM templates are replicated to the subscriber. To synchronize OVF templates and other types of files, the subscriber must initiate the synchronization.
- You can synchronize only OVF templates. If a subscriber initiates synchronization with a published library that contains both VM templates and OVF templates, only the OVF templates are synchronized in the subscribed library. VM templates are synchronized when a publisher library publishes them to its subscribers.

Create a Subscription for a Local Library

Subscriptions enable you to publish library items to a subscriber whenever you want. Create a subscription for a publisher library to control the distribution of templates to the subscriber.

- Verify that publishing is enabled for the library.
- Required privilege:**Content library** > **Create a subscription for a published library** on the content library for which you create a subscription.

When you create a subscription, you can link the publisher library to an existing subscribed library or create a new subscribed library. Creating a subscription to a new subscribed library triggers automatic synchronization. Creating a subscription to an existing library does not trigger automatic synchronization. If you create a subscription to an existing library, the synchronization happens when you publish an item or the entire library.

When you create a subscription to a new subscribed library and you select the option to download library content only when needed, only the metadata for the publisher library contents is downloaded to the associated storage. When the subscriber needs to use a library item, you either publish the item to the subscriber or the subscriber synchronizes the item to download its content to their local storage. For more information about synchronizing an entire library or a library item, see Synchronize the Contents of a Subscribed Library.

1. Select **Menu** > **Content Libraries**.
2. Right-click a local library and select **New Subscription**.

   The **Create Subscription** wizard starts.
3. Select your task.

Task	Steps
Create a new subscription to a new subscribed library	1. On the **Select subscription type** page, select the **Create a new subscription to a new Subscriber library** radio button and click **Next**. 2. On the **Configure subscription** page, configure the subscription and click **Next**. – Select a vCenter Server instance to create the subscribed library in. – Enter a name and description for the new subscribed library. – Select the download method for the new subscribed library. 3. On the **Select folder** page, select a location for the library contents and click **Next**. 4. On the **Select compute resource** page, select the compute resource for the subscribed library and click **Next**. 5. On the **Select storage** page, select a storage location for the subscribed library items and click **Next**. 6. On the **Select network** page, select a network for the synchronization of the subscribed library items and click **Next**. 7. On the **Review** page, review the configuration and click **Finish**.
Create a new subscription to an existing subscribed library	1. On the **Select subscription type** page, select the **Create a new subscription to an existing Subscriber library** radio button and click **Next**. 2. On the **Configure subscription** page, configure the subscription and click **Next**. a. From the **vCenter Server** drop-down menu, select the vCenter Server instance to create the subscription in. A list of all libraries that are subscribed to the publisher and that are in the selected vCenter Server instance appears. b. Select an existing subscribed library from the list.

Task	Steps
	3. On the **Select folder** page, select a location for the subscription and click **Next**. 4. On the **Select compute resource** page, select the compute resource for the subscriber library. 5. On the **Select storage** page, select where to store the contents of the subscriber and click **Next**. 6. On the **Select network** page, select a network for the synchronization of the subscribed library items use and click **Next**. 7. On the **Review** page, review the configuration and click **Finish**.

A new subscription is created. When you go to the **Subscriptions** tab of the local library, you can view a list of all existing subscriptions for the library.

Publish the Contents of a Library to a Subscriber

Publish a library to replicate all VM templates stored in the publisher library to one or multiple subscribers.

Required privileges on the content library:

- **Content library** > **Publish a library to its subscribers**
- **Content library** > **Sync library item**

If the publisher library contains OVF templates and other types of files, publishing the entire library to a subscription only replicates or updates the VM templates.

1. Navigate to the **Content Libraries** list.
2. Select **Menu** > **Content Libraries**.
3. Open a local library by clicking its name.
4. On the **Subscriptions** tab, select the subscriber libraries to update.
5. Click the **Publish** button.
6. In the **Publish Library** pop-up window, click **Publish** to confirm the process.
   A publish task appears in the **Recent Tasks** pane.

All VM templates from the publisher library are published to the selected subscribers.

Publish a Single Template to a Subscription

If you want to replicate a single VM template from a publisher library to a subscriber, you can publish the item, and not the entire library.

Required privileges on the content library:

- **Content library** > **Publish a library item to its subscribers**

- **Content library** > **Sync library item**

1. Navigate to the **Content Libraries** list.
2. Open a local library by clicking its name.
3. On the **Templates** tab, right-click a template of the VM template type and select **Publish**.
4. In the **Publish Template** dialog box, select the subscribers to which to publish the selected template.
5. Click **OK**.
   A publish task appears in the **Recent Tasks** pane.

After the publishing finishes, the item content and metadata are downloaded to the storage of the subscribed library. On the **Templates** tab for the subscription, the value for the item in the **Stored Content Locally** column changes to Yes.

Delete a Subscription

Delete a subscription if you no longer want to share the contents of a publisher library with a subscriber. You might also need to delete a subscription if the corresponding subscribed library has been deleted.

Required privilege: **Content library** > **Delete subscription of a published library** on the library.

If you do not delete a subscription to a deleted subscribed library and you publish content to that subscriber, the task triggers an error. To avoid errors, always delete subscriptions that link to deleted subscribed libraries.

Deleting is a useful option when you need to change a subscription. Because editing is currently not supported, your only choice is to delete the subscription that you want to modify and create a new one.

When you delete a subscription, the respective subscribed library and its contents are not deleted. Deleting a subscription means that you can no longer publish templates to the subscriber. The subscriber can still initiate the synchronization of OVF templates, if any. The subscriber can also continue using the previously synchronized content.

1. Navigate to the **Content Libraries** list.
2. Open a local library by clicking its name.
3. On the **Subscriptions** tab, select one or multiple subscriber libraries from the list.
4. Click the **Delete subscription** button to delete the selected subscriber libraries.

The subscription is deleted and you cannot use the publish function to synchronize the content in the respective subscribed library .

Managing a Subscribed Library

You create a subscribed library to subscribe to a published library. Subscribed libraries are content libraries whose content is connected to the content of a published local library. You cannot add content to a subscribed library, you can only synchronize the content of the subscribed library with the content of the published library.

You can create the subscribed library in the same vCenter Server instance where the published library is, or in a different vCenter Server system. When you create a subscribed library, you can download all the contents of the published library immediately after the subscribed library is created. Alternatively, you can download only the metadata for the items from the published library and later download the full content of only those items that you need.

To ensure that the contents of a subscribed library are up-to-date, the subscribed library automatically synchronizes to the source published library at regular intervals. You can also manually synchronize a single item or an entire subscribed library.

For information about synchronizing an entire subscribed library, see Synchronize a Subscribed Content Library.

For information about synchronizing a library item in a subscribed library, see Synchronize a Library Item in a Subscribed Library.

For information about managing subscriptions and publishing content to a subscriber, see Managing a Publisher Local Library.

When you update VM templates on the publisher library through the check-in and check-out operations, the VM templates are available in the subscriber library after you publish the subscriber library from the **Subscriptions** tab of the publisher.

The vertical timeline view is not available in the subscriber library. You can monitor only the latest version of the VM template.

For information about the VM templates management and the vertical timeline view, see Managing VM Templates.

Download Methods for Synchronization

When you create a subscribed library, you can use the option to download content from the source published library immediately or only when needed to manage your storage space.

- When you synchronize a subscribed library that is configured to download all the contents of the published library immediately, the process synchronizes both the item metadata and the item contents. During synchronization, the library items that are new for the subscribed library are fully downloaded to the subscribed library storage. If some items are deleted from the published library, their contents remain at the storage location of your subscribed library, and you have to manually delete them.
- When you synchronize a subscribed library that is configured to download contents only when needed, the process synchronizes only the metadata for the library items from the published library, and does not download the contents of the items, which saves storage space. If you must use a library item, you need to synchronize that item. Synchronizing a library item downloads the full content of that item to your storage. When you no longer need the item, you can delete the item contents to free storage space.

The supported download methods depend on the source library. For more information, see the following table.

Table 155: Source Objects to Which You Can Subscribe by Creating a Subscribed Library in the vSphere Client

Source Object	Download library content immediately	Download library content when needed
A library running in a vCenter Server 6.x instance	Supported	Supported
A catalog running in a vCloud Director 5.5 and later instance	Supported	Not supported
A third-party library	Supported for third-party libraries that require authentication, if the username of the third-party library is `vcsp`. If the username of the source third-party library is different than `vcsp`, you can subscribe to it by using the VMware vCloud Suite API.	Supported for third-party libraries that require authentication, if the username of the third-party library is `vcsp`. If the username of the source third-party library is different than `vcsp`, you can subscribe to it by using the VMware vCloud Suite API.

Synchronize a Subscribed Content Library

To ensure that your subscribed library displays the latest content of the published library, you can manually initiate a synchronization task.

Required privilege: **Content library** > **Sync subscribed library** on the library.

You can also have subscribed libraries automatically synchronize with the content of the published library. Automatic synchronization requires a lot of storage space, because you download full copies of all the items in a published library.

To enable automatic synchronization, you must change the library settings. For information about changing content library settings, see Edit a Content Library.

1. Navigate to the **Content Libraries** list.
2. Right-click a subscribed library and select **Synchronize**.

A new task for synchronizing the subscribed library appears in the **Recent Tasks** pane. After the task is complete, you can see the updated list with library items on the **Templates** and **Other Types** tabs.

Synchronize a Library Item in a Subscribed Library

To update or download the content of a library item in a subscribed library, you can synchronize the library item.

Required privilege: **Content library** > **Sync library item** on the library item.

When you create a subscribed library, only the metadata for the library contents is downloaded to the associated storage if you selected the option to download library content only when needed. When you need to use a library item, you synchronize it to download its content to your local storage.

When you no longer need the item, you can delete the content of the item to free storage space. You continue to see the item in your subscribed library, but it no longer takes up space on your storage because only the item's metadata remains on the storage. For information about deleting an item, see Delete a Content Library Item.

1. Navigate to the **Content Libraries** list.
2. Select a subscribed library from the list.
3. Synchronize the item that you need to use.
   - On the **Templates** tab, right-click a template, and select **Synchronize Item**.

     Note: Synchronization is not available for VM templates. You can only synchronize OVF templates.
   - On the **Other Types** tab, right-click an item, and select **Synchronize Item**.

After the synchronization finishes, the item content and metadata are downloaded to the storage of the subscribed library. On the **Templates** tab for the subscribed library, the value for the item in the **Stored Content Locally** column changes to Yes.

Populating Libraries with Content

You can populate a content library with VM templates and OVF templates that you can use to provision new virtual machines. You can also add other files to a content library, such as ISO images, scripts, and text files.

You can populate a library with items in several ways.

Import Items to a Content Library

You can add items to a local content library by importing files from your local machine or from a Web server. You can import OVF and OVA templates and other types of files, such as ISO images, certificates, and so on. You can keep the items in the library and share them with other users across multiple vCenter Server instances. You can also use the templates in the content library to deploy new virtual machines and vApps.

Required privilege:**Content library** > **Add library item** and**Content library** > **Update files** on the library.

1. Navigate to the **Content Libraries** list.
2. Right-click a local content library and select **Import Item**.
   The **Import Library Item** dialog box opens.

3. In the **Source** section, choose the source of the item.

Option	Description
Import from a URL	Enter the path to the Web server where the item is. **Note:** You can import either an `.ovf` or `.ova` file. The resulting content library item is of the OVF Template type.
Import from a Local File	Click **Browse** to navigate to the file that you want to import from your local system. You can use the drop-down menu to filter files in your local system. **Note:** You can import either an `.ovf` or `.ova` file. When you import an OVF template, first select the OVF descriptor file (`.ovf`). Next, you are prompted to select the other files in the OVF template, for example the `.vmdk` file. The resulting content library item is of the OVF Template type.

   vCenter Server reads and validates the manifest and certificate files in the OVF package during importing. A warning is displayed in the **Import Library Item** wizard, if certificate issues exist, for example if vCenter Server detects an expired certificate.

   Note: vCenter Server does not read signed content, if the OVF package is imported from an `.ovf` file from your local machine.

4. In the **Destination** section, enter a name and a description for the item.
5. Click **Import**.

In the **Recent Tasks** pane you see two tasks, one about creating a new item in the library, and the second about uploading the contents of the item to the library. After the task is complete, the item appears on the **Templates** tab or on the **Other Types** tab.

Clone a vApp to a Template in a Content Library

You can clone existing vApps to vApp templates in a content library. You can use the vApp templates later to provision new vApps on a cluster or a host in your vSphere inventory. The vApp is exported to a content library in the OVF format.

1. In the vSphere Client, select **Menu** > **VMs and Templates**.
2. Right-click a vApp and select **Clone** > **Clone to Template in Library**.
   The **Clone to Template in Content Library** wizard opens.
3. On the **Basic information** page, configure the content library template and click **Next**.
   a) Select the **New template** radio button.
   b) Enter a name and, optionally, a description for the template.
   c) Optional: Select the **Preserve MAC-addresses on network adapters** check box to preserve the MAC addresses of the network adapters.
   d) Optional: Select **Include extra configuration** to include vApp-related configuration in the template that you clone.
4. On the **Location** page, select a content library to clone the vApp to.
5. On the **Review** page, review the configuration details and click **Finish**

A new task for cloning to OVF package appears in the Recent Tasks pane. After the task finishes, the vApp template appears on the **Templates** tab for the content library.

Use the template to provision vApps on a host or a cluster in your vSphere inventory. See Create New vApp From a Template in a Content Library .

Clone a Virtual Machine or a Virtual Machine Template to a Template in a Content Library

You can add new templates to a content library by cloning virtual machines or virtual machine templates from your vCenter Server inventory to templates in the content library. You can use the content library items later to provision virtual machines on a cluster or a host. You can also update an existing template in the content library by cloning a virtual machine or virtual machine template from the vCenter Server inventory.

Templates are primary copies of virtual machines that you can use to create virtual machines that are ready for use. You can change the template, such as installing additional software in the guest operating system, while preserving the state of the original template. For more information, see Templates in Content Libraries.

When you clone a virtual machine from the vCenter Server inventory as a template to the content library, you can choose what type of content library item to create. You can choose to create a library item of either the VM Template type or OVF Template type.

Important: If you choose to create a VM Template library item, an identical VM template is created in the vCenter Server inventory. For more information about VM templates in a content library, see The VM Template as a Content Library Item .

1. Navigate to the virtual machine or template that you want to clone.
2. Select your task.

Option	Description
Clone a virtual machine	1. Right-click the virtual machine and select **Clone** > **Clone as Template in Library**. The **Clone Virtual Machine To Template** wizard opens. 2. On the **Basic information** page, enter a name and description for the template, select the template type, and select an inventory folder for the template. You can create an OVF Template or VM Template in the content library. 3. On the **Location** page, select a local content library in which you want to add the template. 4. On the **Select a compute resource** page, select the compute resource for the template. 5. On the **Select storage** page, select the storage for the template disk and configuration files. 6. On the **Review** page, review the details and click **Finish** to complete the cloning task.
Clone a virtual machine template	1. Right-click the virtual machine template and select **Clone to Library**. The **Clone to Template in Library** dialog box opens. 2. Select the **Clone as** option. You can create a template or you can choose an existing template to update. 3. From the content libraries list, select the library in which you want to add the template. 4. Enter a name and description for the template. 5. Select the configuration data that you want to include in the template. You can select to preserve the MAC-addresses on the network adapters and include extra configuration. 6. Click **OK**.

A new task for cloning appears in the **Recent Tasks** pane. After the task is complete, the template appears in the **Templates** tab for the content library. You can view the type of template in the **Type** column.

Use the template to create virtual machines on hosts or clusters in the vSphere inventory.

Working with Items in a Library

You can perform various tasks with the items in a content library. You can synchronize an item from a subscribed library to download all its contents and use the item to deploy a virtual machine for example. You can delete items you no longer need to use, and so on.

Each template or other type of file in a content library is a library item. An item can contain a single file or multiple files. For example, when you add an OVF template to the library, you actually upload all the files that are associated with the template, but in the vSphere Client you only see one library item of the OVF Template type.

Update a Content Library Item

Managing and keeping your virtual environment up-to-date might require you to update the content of a library item. For example, you can directly update a template when you want to add a patch to it, instead of deleting the existing template and creating a new one.

Verify that you have the Content Library Administrator role.

Note: You can update only templates from the **OVF and OVA Templates** type. Updating templates from the **VM Templates** type is not supported.

You cannot update the contents of a subscribed library. In local and published libraries, you can update only templates of the OVF Template type.

1. Navigate to the **Content Libraries** list.
2. Click a content library and select the file that you want to update.
   - From the **Templates** tab, right-click a template from the library, and select **Update Item**.
   - From the **Other Types** tab, right-click a file from the library that is not a template, and select **Update Item**.

   The **Update Library Item** dialog box opens.
3. In the **Source** section, select a file to overwrite the item in your library with.

Option	Description
URL	Enter the URL to a web server where the item is stored .
Browse	Navigate to an item that is stored on your local system.

4. Optional: In the **Destination** section, change the name of the item, the description of the item, or both. Click **OK**.

The content of the item is updated. On the **Summary** tab for the item, you can view the time of the last update of the item.

Export an Item from a Content Library to Your Local Computer

You might need to export an item from a content library to your local system.

Required privilege: **Content library** > **Download files** on the library.

Note: You can export only items from the **OVF and OVA Templates** type. Exporting items from the **VM Templates** type is not supported.

1. Navigate to the **Content Libraries** list.
2. Select a content library.
3. Select the type of file you want to export.
   - From the **Templates** tab, right-click a template from the library, and select **Export Item**.
   - From the **Other Types** tab, right-click a file from the library that is not a template, and select **Export Item**.

4. In the **Export Library Item** dialog box click **OK**.
5. If you are exporting an OVF template, you are prompted to save each file associated with the template to the browser download location (for example, `.vmdk` and `.mf` files).

Clone Library Items from One Library to Another Library

You can clone a template from one content library to another in the same vCenter Server instance. The cloned template is an exact copy of the original template.

When cloning a template between libraries, you can select the source library to also be a destination library in the clone wizard.

A subscribed library can be the source of an item you want to clone, but you cannot clone items to a subscribed library. The subscribed libraries are filtered out from the list with destination libraries in the Clone Library Item dialog box. When the source library of an item you want to clone is a subscribed library with the setting to download items only when needed, the item is first downloaded to the source subscribed library and then cloned to the destination library.

1. Navigate to the **Content Libraries** list.
2. Click a content library and click the **Templates** tab.
3. Right-click a template and select **Clone Item**.
   The **Clone Library Item** dialog box opens.
4. Optional: Change the name and notes for the item you clone.
5. From the list of content libraries, select the library in which you want to clone the template and click **OK**.
   You can select the destination library to be the same as the source library if you want to have identical copy of the template in the same library.

A new task for cloning the template appears in the Recent Tasks pane. After the task is complete, a clone of the template appears on the **Templates** tab of the destination content library.
Deploy a virtual machine from template on a host or a cluster in your vSphere inventory.

Edit a Content Library Item

Edit a library item to change its name, description or tag properties.

Required privileges on the library:

- **Content library** > **Update library item**
- **Content library** > **Update local library**

You can edit items only in a local library, regardless of whether it is published or not. Library items in subscribed libraries cannot be modified.

You can edit both VM templates and OVF templates.

1. Navigate to the **Content Libraries** list.
2. Open a local library by clicking its name.
3. Navigate the library item to edit.
   - To edit a template, click the **Templates** tab.
   - To edit another type of file, click the **Other Types** tab.

4. Right-click the item and select your task from the context menu.
   - To edit the description of the item, select **Edit Notes**.
   - To rename the item, select **Rename**.
   - To assign a tag to the item, select **Tags** > **Assign Tag**.
   - To remove a tag from the item, select **Tags** > **Remove Tag**.

Delete a Content Library Item

If you use a subscribed library, and you synchronize it, you can later delete the library from storage but keep the metadata. You can also completely delete a library item such as a template.

Required privileges

Task	Required Privileges
Delete the contents of a library item	**Content library** > **Evict library item**
Delete a library item	**Content library** > **Delete library item**

If a subscribed library is created with the option to download library content only when needed, only metadata for the library items is stored in the associated with the library storage. When you want to use a library item, for example use a VM template to deploy a virtual machine, you have to synchronize the item. Synchronization downloads the entire content to the associated storage.

In the vSphere Client you can delete an item altogether.

1. Select **Menu** > **Content Libraries**.
2. Click a content library, select the type of item, and select the task you want to perform with the item.
3. From the **Templates** tab, right-click a template from the library, and select **Delete**.
4. From the **Other Types** tab, right-click a file from the library that is not a template, and select **Delete**.

Creating Virtual Machines and vApps from Templates in a Content Library

You can deploy virtual machines and vApps from the VM or OVF templates that are stored in a content library.

The library can be a local library to the vCenter Server instance where you want to deploy the VM or the vApp template, or can be a subscribed library to that vCenter Server instance.

The VM Template type is only supported in the vSphere Client. You can deploy virtual machines from VM Templates in a content library only in the vSphere Client.

Note: You can also use the API calls to create and manage VM templates in a content library.

The use of templates results in consistency, compliance, and efficiency when you deploy virtual machines and vApps in your data center.

Deploy a Virtual Machine from an OVF Template in a Content Library

In content libraries, you can use the OVF template, which is either the template of a virtual machine or a vApp, to deploy a virtual machine to a host or a cluster in your vSphere inventory.

1. Navigate to **Menu** > **Content Libraries**.
2. Select a content library and click the **Templates** tab.
3. Right-click an OVF template and select **New VM from This Template**.
   The **New Virtual Machine from Content Library** wizard opens.

4. On the **Select a name and folder** page, enter a name and select a location for the virtual machine.
5. On the **Select a compute resource** page, select a host, a cluster, a resource pool, or a vApp where to run the deployed template, and click **Next**.

   Important:

   If the template that you deploy has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

   If the template that you deploy does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.
6. On the Review details page, verify the template details and click **Next**.
7. On the Select storage page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

Option	Description
Deploy a virtual machine from a template that has vPMem hard disks	1. Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks will be stored on a standard datastore. If you select the **PMem** mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine. If you select the **Hybrid** mode, all PMem virtual disks will remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. 2. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine. 5. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.
Deploy a virtual machine from a template that does not have vPMem hard disks	1. Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. The **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine.

Option	Description
	Thick Provision Eager Zeroed is a type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks. The **Thin Provision** format saves storage space. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it. 2. Select a VM storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Turn on the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.

Note: If you want to use the API calls to deploy an OVF template that contains vPMem hard disks and that has been exported from a content library, consult https://kb.vmware.com/kb/52370.

8. On the Select networks page, select a network for each network adapter in the template and click **Next**.
9. On the Ready to complete page, review the page and click **Finish**.

A new task for creating the virtual machine appears in the Recent Tasks pane. After the task is complete, the new virtual machine is created on the selected resource.

Deploy a Virtual Machine from a VM Template in a Content Library

In the vSphere Client, you can use a content library item of the VM Template type to deploy a virtual machine to a host or cluster in your vSphere environment.

- To access customization options for Windows guest operating systems, Microsoft Sysprep tools must be installed on the system. The Sysprep Tool is built into the Windows Vista and Windows 2008 and later operating systems. For details about this and other customization requirements, see Guest Operating System Customization Requirements.

Important: If the template that you deploy has an NVDIMM device and virtual PMem disks, the destination host or cluster must have an available PMem resourse. Otherwise, you cannot proceed with the task.

If the template that you deploy does not have an NVDIMM device, but has virtual PMem hard disks, the destination host or cluster must have an available PMem resource. Otherwise, all hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

For information about persistent memory and PMem storage, see the *vSphere Resource Management* guide.

For information how to configure the virtual machine hardware options, see Configuring Virtual Machine Hardware and Configuring Virtual Machine Options

Note: If you want to use the API calls to deploy an OVF template that contains vPMem hard disks and that has been exported from a content library, consult https://kb.vmware.com/s/article/52370.

1. Navigate to **Menu** > **Content Libraries**.
2. To open a content library, click its name.
3. On the **Templates** tab, right-click a VM Template and select **New VM from This Template**.
   The **Deploy From VM Template** wizard opens.
4. On the **Select a name and folder** page, enter a name and select a location for the virtual machine.
5. On the **Select a compute resource** page, select a host, a cluster, a resource pool, or a vApp where to run the deployed VM template, and click **Next**.
6. On the **Select storage** page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all virtual disks.

Option	Action
Deploy a virtual machine from a template that has vPMem hard disks	1. Select the type of storage for the template by clicking the **Standard**, the **PMem**, or the **Hybrid** radio button. – If you select the **Standard** mode, all virtual disks are stored on a standard datastore. – If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine. – If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Your choice of a VM storage policy and datastore or datastore cluster affects the Non-PMem disks. 2. From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine. 5. To select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk, enable the **Configure per disk** option. **Note:** To convert a PMem hard disk to a regular one, you can use the **Configure per disk** option , but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.
Deploy a virtual machine from a template that does not have vPMem hard disks	1. Select the disk format for the virtual machine virtual disks. – The **Same format as source** option uses the same disk format as the source virtual machine. – The **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. The space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, or on first write from the virtual machine. – The **Thick Provision Eager Zeroed** format is a type of thick virtual disk that supports clustering features such as Fault Tolerance. The space required for the virtual disk is allocated at creation time. In contrast to the flat format,

Option	Action
	the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks. – The **Thin Provision** format saves storage space. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can extend to the maximum capacity allocated to it. 2. Select a VM storage policy or leave the default one. 3. Select a datastore or a datastore cluster. 4. Enable the **Configure per disk** option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk. **Note:** You can use the **Configure per disk** option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.

7. Click **Next**.
8. On the **Select deploy options** page, apply a customization specification to the virtual machine and click **Next**.

   You can choose to customize the guest operating system or the virtual machine hardware. You can also choose to power on the virtual machine after its creation.

Option	Action
Select an existing specification	Select a customization specification from the list.
Override	To change the guest customization specification for this deployment only, click **Override**, complete the steps in the **Override VM Customization Specification** wizard, and click **OK**.

9. Optional: On the **Customize guest OS** page, select a customization specification to apply to the virtual machine.

   Customizing the guest operating system helps prevent conflicts that can result if you or other users deploy virtual machines with identical settings, such as duplicate computer names.
10. Optional: On the **User settings** page, specify the required settings for the virtual machine.

    This page of the wizard appears only if the selected specification requires additional customization.
11. Optional: On the **Customize hardware** page, configure the virtual machine hardware and options and click **Next**.

    You can leave the defaults and configure the virtual machine hardware and options later.

    Important: If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. You must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.
12. On the **Ready to complete** page, review the information and click **Finish**.

A new task for creating the virtual machine appears in the **Recent Tasks** pane. After the task finishes, the new virtual machine is created on the selected resource.

Create New vApp From a Template in a Content Library

You can use an OVF template to create a new vApp on a host or a cluster in your vSphere inventory.

1. Navigate to **Menu** > **Content Libraries**.
2. Open a content library by clicking its name, and click the **Templates** tab.
3. Right-click a template of a vApp and select **New vApp from This Template**.
   The **New vApp from Content Library** wizard opens.
4. On the **Select a name and folder** page, enter a name and select a location for the vApp, and click **Next**.
5. On the **Select a compute resource** page, select a host, a cluster, a resource pool, or a vApp to deploy the vApp to and click **Next**.
6. On the **Review detail**s page, verify the template details and click **Next**.
7. On the **Select storage** page, select disk format and a storage resource for the vApp.
8. On the **Select networks** page, select a destination network for each source network.
9. On the **Ready to complete** page, review the configurations you made for the vApp, and click **Finish**.

A new task for creating the vApp appears in the **Recent Tasks** pane. After the task is complete, the new vApp is created.

Managing VM Templates

In vSphere 7.0, you can manage VM templates in an efficient and flexible manner. You can edit the contents of the VM templates by checking them out, making the necessary changes, and checking them in.

You can track history of changes over time by using the vertical timeline view. The vertical timeline view provides you with detailed information about the different VM template versions, the updates that privileged users have made, and when the last change was made. By using the vertical timeline, you can revert VM templates back to their previous state or delete the previous version of a VM template.

In addition, you can deploy a virtual machine from the latest version of the VM template without any disruptions while it is checked out for update. You can update the virtual machine and check it back in into the same VM template.

Templates in Content Libraries

Templates are primary copies of virtual machines that you can use to deploy virtual machines that are customized and ready for use. Templates promote consistency throughout your vSphere environment. You can use the content library to store and manage templates of virtual machines and vApps. You can use VM templates and vApp templates to deploy virtual machines and vApps to a destination object, such as a host or a cluster.

Content libraries support two types of templates, the OVF Template type and the VM Template type.

In a content library, you can store and manage virtual machine templates as OVF templates or VM templates. vApps are always converted to OVF templates in the content library.

VM Templates in Content Libraries

A VM template is a template of a virtual machine. You create a VM template by cloning a virtual machine into a template.

OVF Templates in Content Libraries

In a content library, an OVF template is either a template of a virtual machine, or a template of a vApp. When you clone a virtual machine into a template in a content library, you choose whether to create an OVF template or a VM template. However, if you clone a vApp into a template in a content library, the resulting content library item is always an OVF

template. Because the OVF format is actually a set of files, if you export the template, all the files in the OVF template library item (`.ovf`, `.vmdk`, `.mf`) are saved to your local system.

The VM Template as a Content Library Item

VM Templates in the Content Library and VM Templates in the vCenter Server Inventory

When you create a VM template in a content library, the library item is backed by a VM template in the vCenter Server inventory. The content library item and the corresponding inventory object are related in the following ways.

- If you convert the VM template in the vCenter Server inventory to a virtual machine, the corresponding VM template library item is also deleted.
- If you rename the VM template in the vCenter Server, the corresponding VM template library item is also renamed.
- If you rename the VM template library item the associated VM template in the vCenter Server inventory is also renamed.
- If you delete the VM template in the vCenter Server inventory, the corresponding VM template library item is also deleted.
- If you delete the VM template library item, the associated VM template in the vCenter Server inventory is also deleted.

VM Templates and OVF Templates in the Content Library

You can use both VM templates and OVF templates to deploy new virtual machines in your vSphere environment. However, the two types of templates have different properties and support different deployment options.

See the following table for a detailed list of the differences between VM templates and OVF templates in a content library.

Table 156: VM Templates and OVF Templates Properties

Property	VM Templates in Content Library	OVF Templates in Content Library
Datastore	VM templates can be stored on any datastore that you have privileges to. **Note:** VM templates cannot be stored in a library that uses NFS or SMB storage.	OVF templates can only be stored on the datastore that is associated with the content library.
Footprint	The default one.	Compressed or Thin.
Host/Datastore Maintenance Mode	When the host becomes inaccessible, VM templates are automatically migrated to another host.	When either the host or the datastore becomes inaccessible, you must manually migrate the OVF templates to another host or datastore.
Associated with a Host	Yes.	No.
Storage DRS	Supported.	Not supported.
Cross-vendor Compatibility	Not supported.	Supported.
Software License Agreement	Not supported.	Supported.
Encryption	Supported. You can create encrypted VM templates.	Not supported. While OVF templates cannot be encrypted themselves, you can still deploy an encrypted virtual machine from an OVF template.

Property	VM Templates in Content Library	OVF Templates in Content Library
Deployment Options	During the deployment of a VM template, hardware customization and guest OS customization are both supported.	During the deployment of an OVF template, only guest OS customization is supported. Hardware customization is not supported.

The supported operations on a content library template are different depending on the template type. You can edit the settings for both OVF and VM templates. However, you can update, export, and clone a template only if it is an OVF template.

Check Out a Virtual Machine from a Template

In the vSphere Client, you can edit the VM templates and monitor the changes that have been made by other privileged users. You can perform the checkout operation to update a virtual machine from the VM template. During this process, the VM template is not available for checkout from other users, but they can deploy a virtual machine from the VM template without any disruptions.

Verify that you have the following privileges:

- **Content library** > **Check out a template**
- **Resource** > **Assign virtual machine to resource pool**
- **Datastore** > **Allocate space**
- **Virtual machine** > **Inventory** > **Create from existing**
- **Virtual machine** > **Configuration** > **Set annotation**
- If you want to power on the checked out virtual machine, verify that you have the**Virtual machine** > **Interaction** > **Power On** privilege.

When you check out a VM template, you cannot convert the virtual machine to a template or migrate the virtual machine to a different vCenter Server inventory.

1. To check out a VM template

Option	Action
From a content library	1. Navigate to **Menu** > **Content Libraries**. 2. To open a local library, click its name. 3. On the **Templates** tab, select a VM template and click the **Check out VM from this template** button.
From the vSphere Client inventory	1. Navigate to **Menu** > **VMs and Templates** and click the VM template. 2. Click the **Versioning** tab and in the vertical timeline view, click **Check out VM from this template**.

   The **Check out VM from VM Template** dialog box opens.

2. On the **Name and location** page, enter a virtual machine name, select the virtual machine location, and click **Next**.
3. On the **Select compute resource** page, select the compute resource for the checked out virtual machine and click **Next**.
4. On the **Review** page, review the configuration.
5. Choose whether to power on the virtual machine after checkout by selecting the **Power on VM after checkout** check box.
6. Click **Finish**.

The checked out virtual machine appears in the selected location marked with a blue circle icon. You can perform the necessary configuration changes.

After you complete the virtual machine updates, you can check in the virtual machine back to the template.

Check In a Virtual Machine to a Template

After you check out a virtual machine from a template and update the virtual machine, you must check the virtual machine back into the VM template. When you check in the virtual machine to a template, you create a new version of the VM template containing the updated state of the virtual machine.

Verify that the virtual machine is powered off or suspended. You cannot check in a powered on virtual machine to a VM template.

Required privileges:

- **Content library** > **Check in a template**

When you check in the virtual machine to the VM template, you allow the deployment of the last changes that you make to the virtual machine.

1. To check in a virtual machine to a template:

Option	Action
From a content library	1. Navigate to **Menu** > **Content Libraries**. 2. To open a content library, click its name. 3. On the **Templates** tab, select a VM template and click **Check in VM to template**.
From the vSphere Client inventory	1. Navigate to **Menu** > **VMs and Templates** and click the VM template. 2. Click the **Versioning** tab and in the vertical timeline view, click **Check in VM to template**.

   The **Check in VM** dialog box opens.
2. To describe the change, enter a comment in **Check in notes** .
3. Click **Check in**.

The updated version of the VM template appears in the vertical timeline. You can see the check-in comment, the name of the user who made the changes, and the date of the change.

Discard a Checked Out Virtual Machine

If you check out a VM template and make no updates to the virtual machine or perform an update that you do not want to keep, you can discard the checked out virtual machine. Each time you check in the virtual machine back to the template,

you create a new version of the VM template. You can discard the checked out virtual machine to avoid creating new versions or to prevent other users from using a faulty version.

Required privileges:

- **Virtual machine** > **Inventory** > **Delete**

1. To discard a checked out virtual machine:

Option	Action
From a content library	1. Navigate to **Menu** > **Content Libraries**. 2. To open a local library, click its name. 3. On the **Templates** tab, select a VM template. 4. From the vertical timeline, click the horizontal ellipsis icon (•••) that appears in the checked out VM template box and select **Discard Checked Out VM**.
From the vSphere Client inventory	1. Navigate to **Menu** > **VMs and Templates** and click the VM template. 2. Click the **Versioning** tab in the vertical timeline. 3. Click the horizontal ellipsis icon (•••) that appears in the checked out VM template box, and select **Discard Checked Out VM**.

   The **Discard Checked Out VM** dialog box opens.

2. To delete the checked out virtual machine and discard all changes, click **Discard**.

You deleted the virtual machine from the inventory and discarded all changes.

Revert to a Previous Version of a Template

If the latest VM template contains changes that you no longer want to keep or you made a mistake during your last checkin, you can revert the VM template to the previous version.

Required privileges:

- **Content library** > **Check in a template**

1. To revert to a previous version of a template:

Option	Action
From a content library	1. Navigate to **Menu** > **Content Libraries**. 2. To open a local library, click its name. 3. On the **Templates** tab, select a VM template.
From the vSphere Client inventory	1. Navigate to **Menu** > **VMs and Templates** and click the VM template. 2. Click the **Versioning** tab.

2. From the vertical timeline, navigate to the previous state of the VM template, click the horizontal ellipsis icon (•••), and select **Revert to This Version**.

   The **Revert to Version** dialog box opens.

3. Enter a reason for the revert operation and click **Revert**.

The VM template that you revert to becomes the current VM template.

Delete a Previous Version of a VM Template

Delete a previous version of a VM template if you no longer want to allow the use of the template. Deleting a VM template removes the template and its content from the inventory.

Required privileges:

- **Content Library** > **Delete library item**

1. To delete a previous version of a template:

Option	Action
From a content library	1. Navigate to **Menu** > **Content Libraries**. 2. To open a local library, click its name. 3. On the **Templates** tab, select a VM template.
From the vSphere Client inventory	1. Navigate to **Menu** > **VMs and Templates** and click the VM template. 2. Click the **Versioning** tab.

2. From the vertical timeline, navigate to the previous state of the VM template, click the horizontal ellipsis icon (•••), and select **Delete Version**.

   The **Confirm Delete** dialog box opens.

3. To delete permanently the VM template and its contents, click **Yes**.

Configuring Virtual Machine Hardware

You can add or configure most virtual machine hardware settings during virtual machine creation or configure those settings after you create the virtual machine and install the guest operating system.

When you configure the virtual machine hardware, you can view the existing hardware configuration and add or remove hardware. You can change nearly every setting that was selected during virtual machine creation.

Virtual Machine Compatibility

When you create a virtual machine or upgrade an existing virtual machine, you use the virtual machine compatibility setting to select the ESXi host versions that the virtual machine can run on.

The compatibility setting determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. Virtual hardware includes BIOS and EFI, available virtual PCI slots, maximum number of CPUs, maximum memory configuration, and other characteristics. New virtual hardware capabilities are typically released once a year with major or minor releases of vSphere.

Each virtual machine compatibility level supports at least five major or minor vSphere releases. For example, a virtual machine with ESXi 6.0 and later compatibility can run on ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, ESXi 7.0 Update 3.

Table 157: Virtual Machine Compatibility Options

Compatibility	
ESXi 7.0 Update 3 and later	This virtual machine (hardware version 19) is compatible with ESXi 7.0 Update 3 and later.
ESXi 7.0 Update 2 and later	This virtual machine (hardware version 19) is compatible with ESXi 7.0 Update 2 and ESXi 7.0 Update 3.
ESXi 7.0 Update 1 and later	This virtual machine (hardware version 18) is compatible with ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3.

Compatibility	
ESXi 7.0 and later	This virtual machine (hardware version 17) is compatible with ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3.
ESXi 6.7 Update 2 and later	This virtual machine (hardware version 15) is compatible with ESXi 6.7 Update 2, ESXi6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3.
ESXi 6.7 and later	This virtual machine (hardware version 14) is compatible with ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3.
ESXi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3.
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0, ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3.

The compatibility setting that appears in the **Compatible with** drop-down menu is the default for the virtual machine that you are creating. The following factors determine the default virtual machine compatibility:

- The ESXi host version on which the virtual machine is created.
- The inventory object that the default virtual machine compatibility is set on, including a host, cluster, or data center.

You can accept the default compatibility or select a different setting. It is not always necessary to select the latest ESXi host version. Selecting an earlier version can provide greater flexibility and is useful in the following situations:

- To standardize testing and deployment in your virtual environment.
- If you do not need the capabilities of the latest host version.
- To maintain compatibility with older hosts.

When you create a virtual machine, consider the environment that the virtual machine runs in and weigh the benefits of different compatibility strategies. Consider your options for these scenarios, which demonstrate the flexibility inherent with each virtual machine compatibility selection.

Objects in Environment	Compatibility	Results
Cluster with ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3 hosts	ESXi 6.5 and later	This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 6.7 and later.
Cluster with ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3 hosts	ESXi 6.7 and later	This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 7.0 and later. A virtual machine with such compatibility cannot run on ESXi 6.5.
Cluster with ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3 hosts	ESXi 7.0 and later	This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 7.0 Update 1 and later. A virtual machine with such compatibility cannot run on ESXi 6.7 and earlier.
Cluster with ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3 hosts	ESXi 7.0 Update 1 and later	This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 7.0 Update 2 and later. A virtual machine with such compatibility cannot run on ESXi 7.0 and earlier.

Objects in Environment	Compatibility	Results
Cluster with ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3 hosts	ESXi 7.0 Update 2 and later	This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 7.0 Update 3 and later. A virtual machine with such compatibility cannot run on ESXi 7.0 Update 1 and earlier.
Cluster with ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, ESXi 7.0 Update 2, and ESXi 7.0 Update 3 hosts	ESXi 7.0 Update 3 and later	This provides access to the latest virtual hardware features and ensures best performance. However, a virtual machine with such compatibility cannot run on ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 7.0 Update 1, or ESXi 7.0 Update 2.

Set the Default Compatibility for Virtual Machine Creation

You can set the default compatibility for virtual machine creation on the host, cluster, or data center. These options ensure that when virtual machines are added to an existing vSphere environment, they are compatible with the host versions that reside there.

Required privileges:

- On the host or cluster: **Host** > **Inventory** > **Modify cluster**
- On the data center: **Datacenter** > **Reconfigure datacenter**

The following conditions apply:

- To set the default compatibility on the cluster, the cluster must contain hosts that are connected and not in maintenance mode.
- A default compatibility setting on the host overrides a default cluster or data center setting.
- A default compatibility setting on the cluster overrides a default data center setting.

Select a host, cluster, or data center in the inventory.

Option	Action
Host	1. Click the **Configure** tab, and under **Virtual Machines**, select **Default VM Compatibility**. 2. Click **Edit**. The **Edit Default VM Compatibility** dialog box opens. 3. From the **Compatible with** drop-down menu, select the compatibility and click **OK**. **Note:** You can set the compatibility only on hosts that are not part of a cluster.
Cluster	1. Click the **Configure** tab and under **Configuration**, select **General**. 2. In the **Default VM Compatibility** section, click **Edit**. 3. From the **Compatible with** drop-down menu, select the compatibility and click **OK**. When you change the compatibility for a cluster, the compatibility for all hosts in the cluster changes as well.
Data Center	1. Right-click the data center and select **Edit Default VM Compatibility**. 2. From the **Compatible with** drop-down menu, select the compatibility and click **OK**.

When you create a virtual machine on one of these objects, the default compatibility setting is used.

Schedule a Compatibility Upgrade for a Single Virtual Machine

The compatibility level determines the virtual hardware available to a virtual machine, which corresponds to the physical hardware available on the host machine. You can upgrade the compatibility to make the virtual machine compatible with the latest version of the host.

- Create a backup or snapshot of the virtual machines.
- Upgrade to the latest version of VMware Tools. On Microsoft Windows virtual machines, if you upgrade the compatibility level before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ESXi host on a VMFS5, or NFS datastore.
- Verify that the virtual machine is stored on VMFS5 or NFS datastores.

To schedule an upgrade for multiple virtual machines, see Schedule a Compatibility Upgrade for a Virtual Machine.

1. Right-click a virtual machine and select **Compatibility** > **Schedule VM Compatibility Upgrade**.
2. In the **Schedule VM Compatibility Upgrade** dialog box, confirm that you want to schedule a compatibility upgrade by clicking **Yes**.
3. From the **Compatible with** drop-down menu, select the compatibility to upgrade to.

   The virtual machine compatibility is upgraded the next time you restart the virtual machine.
4. Optional: To upgrade the compatibility when you do regularly scheduled guest maintenance, select **Only upgrade after normal guest OS shutdown**.

The virtual machine compatibility is upgraded and the new version appears on the virtual machine Summary tab.

Change the Default Virtual Machine Compatibility Setting

The virtual machine compatibility determines the virtual hardware available to the virtual machine. You can schedule a compatibility upgrade to make a virtual machine compatible with newer versions of ESXi.

- Create a backup or snapshot of the virtual machines. See Using Snapshots To Manage Virtual Machines.
- Upgrade to the latest version of VMware Tools. If you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machines are stored on VMFS3, VMFS5 or NFS datastores.
- Verify that the compatibility settings for the virtual machines are not the latest supported version.
- Determine the ESXi versions that you want the virtual machines to be compatible with. See Virtual Machine Compatibility.

You can change the compatibility of an individual virtual machine by upgrading its compatibility or scheduling an compatibility upgrade.

You can also change the default compatibility setting for the host, cluster, or data center.

1. Optional: To determine the compatibility setting of a virtual machine, select the virtual machine in the inventory and click the **Summary** tab.
2. Select your task.

Client	Tasks
vSphere Client	• Change the default compatibility setting of a virtual machine. – Right-click a virtual machine and click **Compatibility** > **Upgrade VM Compatibility**. – Right-click a virtual machine and click **Compatibility** > **Schedule VM Compatibility Upgrade**.

Hardware Features Available with Virtual Machine Compatibility Settings

The virtual machine compatibility setting determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. You can review and compare the hardware available for different compatibility levels to help you determine whether to upgrade the virtual machines in your environment.

You can add up to ten PVRDMA network adapters to a virtual machine when using vSphere 7.0 Update 2 and later.

Table 158: Supported Features for Virtual Machine Compatibility

Feature	ESXi 7.0 Update 3 and later	ESXi 7.0 Update 2 and later	ESXi 7.0 Update 1 and later	ESXi 7.0 and later	ESXi 6.7 Update 2 and later	ESXi6.7 and later	ESXi 6.5 and later .	ESXi 6.0 and later
Hardware version	19	19	18	17	15	14	13	11
Maximum memory (GB)	24560	24560	24560	6128	6128	6128	6128	4080
Maximum number of logical processors	768	768	768	256	256	128	128	128
Maximum number of cores (virtual CPUs) per socket	64	64	64	64	64	64	64	64
Maximum SCSI controllers	4	4	4	4	4	4	4	4
Bus Logic controllers	Y	Y	Y	Y	Y	Y	Y	Y
LSI Logic controllers	Y	Y	Y	Y	Y	Y	Y	Y
LSI Logic SAS controllers	Y	Y	Y	Y	Y	Y	Y	Y

Feature	ESXi 7.0 Update 3 and later	ESXi 7.0 Update 2 and later	ESXi 7.0 Update 1 and later	ESXi 7.0 and later	ESXi 6.7 Update 2 and later	ESXi6.7 and later	ESXi 6.5 and later .	ESXi 6.0 and later
VMware Paravirtual controllers	Y	Y	Y	Y	Y	Y	Y	Y
SATA controllers	4	4	4	4	4	4	4	4
NVMe controllers	4	4	4	4	4	4	4	N
Virtual SCSI disk	Y	Y	Y	Y	Y	Y	Y	Y
SCSI passthrough	Y	Y	Y	Y	Y	Y	Y	Y
SCSI hot add support	Y	Y	Y	Y	Y	Y	Y	Y
IDE nodes	Y	Y	Y	Y	Y	Y	Y	Y
Virtual IDE disk	Y	Y	Y	Y	Y	Y	Y	Y
Virtual IDE CD-ROMs	Y	Y	Y	Y	Y	Y	Y	Y
IDE hot add support	N	N	N	N	N	N	N	N
Maximum NICs	10	10	10	10	10	10	10	10
PCNet32	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet2	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet3	Y	Y	Y	Y	Y	Y	Y	Y
E1000	Y	Y	Y	Y	Y	Y	Y	Y
E1000e	Y	Y	Y	Y	Y	Y	Y	Y
USB 1.x and 2.0	Y	Y	Y	Y	Y	Y	Y	Y
USB 3.1 SuperSpeed	Y	Y	Y	Y	Y	Y	Y	Y
USB 3.1 SuperSpeedPlus	Y	Y	Y	Y	N	N	N	N
Maximum video memory (MB)	256	256	256	128	128	128	128	128

Feature	ESXi 7.0 Update 3 and later	ESXi 7.0 Update 2 and later	ESXi 7.0 Update 1 and later	ESXi 7.0 and later	ESXi 6.7 Update 2 and later	ESXi6.7 and later	ESXi 6.5 and later .	ESXi 6.0 and later
Maximum 3D graphics memory (GB)	8	8	8	4	2	2	2	2
SVGA displays	10	10	10	10	10	10	10	10
SVGA 3D hardware acceleration	Y	Y	Y	Y	Y	Y	Y	Y
VMCI	Y	Y	Y	Y	Y	Y	Y	Y
PCI passthrough	16	16	16	16	16	16	16	16
Dynamic DirectPath	Y	Y	Y	Y	N	N	N	N
PCI Hot add support	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Precision Clock device	Y	Y	Y	Y	N	N	N	N
Virtual Watchdog Timer device	Y	Y	Y	Y	N	N	N	N
Virtual SGX device	Y	Y	Y	Y	N	N	N	N
Nested HV support	Y	Y	Y	Y	Y	Y	Y	Y
vPMC support	Y	Y	Y	Y	Y	Y	Y	Y
Serial ports	32	32	32	32	32	32	32	32
Parallel ports	3	3	3	3	3	3	3	3
Floppy devices	2	2	2	2	2	2	2	2
PVRDMA	10	10	1	1	1	1	1	0
PVRDMA native endpoint (w/o vMotion)	Y	Y	Y	N	N	N	N	N

Feature	ESXi 7.0 Update 3 and later	ESXi 7.0 Update 2 and later	ESXi 7.0 Update 1 and later	ESXi 7.0 and later	ESXi 6.7 Update 2 and later	ESXi6.7 and later	ESXi 6.5 and later .	ESXi 6.0 and later
PVRDMA native endpoint (with vMotion)	Y	Y	N	N	N	N	N	N
NVDIMM controller	1	1	1	1	1	1	N	N
NVDIMM device	64	64	64	64	64	64	N	N
Virtual I/O MMU	Y	Y	Y	Y	Y	Y	N	N
Virtual TPM	Y	Y	Y	Y	Y	Y	N	N
Microsoft VBS	Y	Y	Y	Y	Y	Y	N	N
Direct3D 10.1	Y	Y	Y	Y	N	N	N	N
Direct3D 11.0	Y	Y	N	N	N	N	N	N
AMD SEV-ES	Y	Y	Y	N	N	N	N	N

Virtual CPU Configuration

You can add, change, or configure CPU resources to improve virtual machine performance. You can set most of the CPU parameters when you create virtual machines or after the guest operating system is installed. Some actions require that you power off the virtual machine before you change the settings.

VMware uses the following terminology. Understanding these terms can help you plan your strategy for CPU resource allocation.

CPU
The CPU, or processor, is the component of a computer system that performs the tasks required for computer applications to run. The CPU is the primary element that performs the computer functions. CPUs contain cores.

CPU Socket
A CPU socket is a physical connector on a computer motherboard that connects to a single physical CPU. Some motherboards have multiple sockets and can connect multiple multicore processors (CPUs).

Core
A core contains a unit containing an L1 cache and functional units needed to run applications. Cores can independently run applications or threads. One or more cores can exist on a single CPU.

Resource sharing
Shares specify the relative priority or importance of a virtual machine or resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when the two virtual machines are competing for resources.

Resource allocation
You can change CPU resource allocation settings, such as shares, reservation, and limit, when available resource capacity does not meet demands. For example, if at year end, the workload on

	accounting increases, you can increase the accounting resource pool reserve.
vSphere Virtual Symmetric Multiprocessing (Virtual SMP)	Virtual SMP or vSphere Virtual Symmetric Multiprocessing is a feature that enables a single virtual machine to have multiple processors.

Virtual CPU Limitations

The maximum number of virtual CPUs that you can assign to a virtual machine is 768. The number of virtual CPUs depends on the number of logical CPUs on the host, and the type of guest operating system that is installed on the virtual machine.

Be aware of the following limitations:

- A virtual machine cannot have more virtual CPUs than the number of logical cores on the host. The number of logical cores is equal to the number of physical cores if hyperthreading is deactivated or two times that number if hyperthreading is activated.
- If a running virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a running virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.
- The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.
- Not every guest operating system supports Virtual SMP, and guest operating systems that support this functionality might support fewer processors than are available on the host. For information about Virtual SMP support, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Configuring Multicore Virtual CPUs

VMware multicore virtual CPU support lets you control the number of cores per virtual socket in a virtual machine. This capability lets operating systems with socket restrictions use more of the host CPU cores, which increases overall performance.

Important: When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Using multicore virtual CPUs can be useful when you run operating systems or applications that can take advantage of only a limited number of CPU sockets.

You can configure a virtual machine with ESXi 7.0 Update 1 and later compatibility to have up to 768 virtual CPUs. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical CPUs means the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 virtual CPUs.

You configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single-core CPU, dual-core CPU, tri-core CPU, and so on. Your selection determines the number of sockets that the virtual machine has.

The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

For more information about multicore CPUs, see the *vSphere Resource Management* documentation.

Enable CPU Hot Add

By default, you cannot add CPU resources to a virtual machine when the virtual machine is powered on. The CPU hot add option lets you add CPU resources to a running virtual machine.

- Verify that the virtual machine is configured as follows.
  - Latest version of VMware Tools installed.
  - Guest operating system that supports CPU hot add.
  - Virtual machine compatibility is ESX/ ESXi 4.x or later.
  - Virtual machine is powered off.
- Required privileges: **Virtual Machine** > **Configuration** > **Settings**

The following conditions apply.

- For best results, use virtual machines that are compatible with ESXi 5.0 or later.
- Hot adding multicore virtual CPUs is supported only with virtual machines that are compatible with ESXi 5.0 or later.
- If a virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs to be over 128. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.
- Not all guest operating systems support CPU hot add. You can deactivate these settings if the guest operating system is not supported.
- To use the CPU hot add feature with virtual machines that are compatible with ESXi 4.x and later, set the **Number of cores per socket** to 1.
- Adding CPU resources to a running virtual machine with CPU hot add enabled disconnects and reconnects all USB passthrough devices that are connected to that virtual machine.

Note: If the ESXi host is of version 7.0 Update 2 and earlier, hot-adding virtual CPUs to a virtual machine with NVIDIA vGPU requires that the ESXi host have a free vGPU slot. Starting with vSphere 7.0 Update 3, the source host does not require to a have a free vGPU slot.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU**, and select **Enable CPU Hot Add**.
3. Click **OK**.

You can now add CPUs even if the virtual machine is powered on.

Change the Number of Virtual CPUs

A virtual machine with ESXi 7.0 Update 1 and later compatibility can have up to 768 virtual CPUs. You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hot add is enabled, you can increase the number of virtual CPUs while the virtual machine is running.

- If CPU hot add is not enabled, power off the virtual machine before adding virtual CPUs.
- To hot add multicore CPUs, verify that the virtual machine is compatible with ESXi 5.0 and later.
- Verify that you have the **Virtual Machine** > **Configuration** > **Change CPU Count** privilege.

Virtual CPU hot add is supported for virtual machines with multicore CPU support and ESXi 5.0 and later compatibility. When the virtual machine is powered on and CPU hot add is enabled, you can hot add virtual CPUs to the running virtual machine. You can add only multiples of the number of cores per socket.

If a virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.

The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

Important: When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU**.
3. From the **CPU** drop-down menu, select the number of cores.
4. From the **Cores Per Socket** drop-down menu, select the number of cores per socket and click **OK**.

Expose VMware Hardware Assisted Virtualization

You can expose full CPU virtualization to the guest operating system so that applications that require hardware virtualization can run on virtual machines without binary translation or paravirtualization.

Note: VMware does not support running third-party hypervisors on ESXi with the exception of specifically defined and documented functionality. Currently, this is limited to Microsoft Hyper-V, strictly for VBS only and not for virtualizing multiple VMs.

For more information, see the VMware KB article at https://kb.vmware.com/s/article/2009916.

- Verify that the virtual machine compatibility is ESXi 5.1 and later.
- Intel Nehalem Generation (Xeon Core i7) or later processors or AMD Opteron Generation 3 (Greyhound) or later processors.
- Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware assisted virtualization is possible.
- Required Privileges: **Virtual machine** > **Configuration** > **Change Settings** set on the vCenter Server system.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU**, and select **Expose hardware assisted virtualization to the guest OS**.
3. Click **OK**.

   The **Configure** tab refreshes, and the Nested Hypervisor CPU option shows **Enabled.**

Activate Virtual CPU Performance Counters

You can use performance tuning tools in the guest operating system for software profiling. You can identify and improve processor performance problems. This capability is useful for software developers who optimize or debug software that runs in the virtual machine.

- Verify that the virtual machine compatibility is ESXi 5.1 and later.
- Verify that the virtual machine is turned off.
- Verify that Intel Nehalem Generation (Xeon Core i7) or later processors or AMD Opteron Generation 3 ("Greyhound") or later processors are installed.
- Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware-assisted virtualization is possible.
- Required Privileges:**Virtual machine** > **Configuration** > **Change Settings** is set on the vCenter Server system.

The following conditions apply:

- If virtual CPU performance counters are enabled, you can migrate the virtual machine only to hosts that have compatible CPU performance counters.
- If an ESXi host's BIOS uses a performance counter or if Fault Tolerance is enabled, some virtual performance counters might not be available for the virtual machine to use.

Note: If a virtual machine resides on an ESXi host in an EVC cluster, CPU counters are not supported for virtual machine creation or editing. You must deactivate CPU performance counters.

For a list of virtualized Model-Specific Registers (MSRs), see the VMware knowledge base article at http://kb.vmware.com/kb/2030221.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU** and select the **Enable virtualized CPU performance counters** check-box.
3. Click **OK**.

Configure Processor Scheduling Affinity

The **Scheduling Affinity** option gives you detailed control over how virtual machine CPUs are distributed across the host's physical cores. The option supports hyperthreading if hyperthreading is enabled. ESXi generally manages processor scheduling well, even when hyperthreading is enabled. These settings are useful only for fine-tuning critical virtual machines.

- Verify that the virtual machine is turned off.
- Verify that the virtual machine does not reside in a DRS cluster.
- Verify that the host has more than one physical processor core.
- Privileges: **Virtual machine** > **Configuration** > **Change resource**

Using CPU affinity, you can assign a virtual machine to a specific processor. This assignment allows you to restrict the assignment of virtual machines to a specific available processor in multiprocessor systems.

This setting does not appear for virtual machines in a DRS cluster or when the host has only one processor core and no hyperthreading.

For potential issues with CPU affinity, see the *vSphere Resource Management* documentation.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU**, and enter a comma-separated list of hyphenated processor ranges in the **Scheduling Affinity** text box.
   For example, "0,4-7" would indicate affinity with CPUs 0,4,5,6, and 7. Selecting all processors is identical to selecting no affinity. You must provide at least as many processor affinities as you have virtual CPUs.
3. Click **OK**.

Activate IO/MMU Virtualization Settings

ESXi can determine whether a virtual machine needs hardware support for virtualization. ESXi makes this determination based on the processor type and the virtual machine. Overriding the automatic selection can provide better performance for some use cases.

Important: Modern x86 processors can fully support virtualized workloads without software assistance. So, the CPU/MMU Virtualization setting has been deprecated in ESXi 6.7 and later. The CPU/MMU Virtualization setting is available only for virtual machines with ESXi 6.5 and earlier compatibility.

You can use software MMU when your virtual machine runs heavy workloads, such as Translation Lookaside Buffers (TLBs) intensive workloads that have significant impact on the overall system performance. However, software MMU has

a higher overhead memory requirement than hardware MMU. So, to support software MMU, the maximum overhead supported for virtual machine limit in the VMkernel must be increased.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU**, and select the **Enabled** check box to activate the I/O MMU options for a virtual machine.

   Note: To take advantage of all features that virtual hardware version 13 provides, use the default hardware MMU setting.
3. Click **OK**.

Virtual Memory Configuration

You can add, change, or configure virtual machine memory resources or options to enhance virtual machine performance. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. Some actions require that you power off the virtual machine before changing the settings.

The memory resource settings for a virtual machine determine how much of the host's memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size. ESXi hosts limit the memory resource use to the maximum amount useful for the virtual machine, so that you can accept the default of Unlimited memory resources.

Change the Memory Configuration

You can reconfigure the amount of memory allocated to a virtual machine to enhance performance.

Verify that you have the **Virtual machine** > **Configuration** > **Change Memory** privilege on the virtual machine.

Minimum memory size is 4 MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96 MB of RAM or they cannot power on.

Maximum memory size for virtual machines that use BIOS firmware is 24560 GB. You must use EFI firmware for virtual machines with memory size greater than 6128 GB.

Maximum memory size for a virtual machine depends on the physical memory of the ESXi host and the virtual machine compatibility settings.

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance. The maximum for best performance represents the threshold above which the physical memory of the ESXi host is insufficient to run the virtual machine at full speed. This value fluctuates as conditions on the host change, for example, as virtual machines are powered on or off.

The memory size must be a multiple of 4 MB.

Table 159: Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 7.0 Update 3	ESXi 7.0 Update 3 and later	24560 GB
ESXi 7.0 Update 2	ESXi 7.0 Update 2 and later	24560 GB
ESXi 7.0 Update 1	ESXi 7.0 Update 1 and later	24560 GB
ESXi 7.0	ESXi 7.0 and later	6128 GB
ESXi 6.7 Update 2	ESXi 6.7 Update 2 and later	6128 GB
ESXi 6.7	ESXi 6.7 and later	6128 GB

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 6.5	ESXi 6.5 and later	6128 GB
ESXi 6.0	ESXi 6.0 and later	4080 GB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a virtual machine with ESXi 6.0 and later compatibility running on ESXi 6.5 is restricted to 4080 GB.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Memory** and change the memory configuration.
   a) In the **Memory** text box, enter the amount of RAM to assign to the virtual machine.
   b) Select whether the memory is specified in MB, GB or TB.
3. Click **OK**.

Allocate Memory Resources

You can change the amount of memory resources allocated to a virtual machine by using the shares, reservations, and limits settings. The host determines the appropriate amount of physical RAM to allocate to virtual machines based on these settings. You can assign a high or low shares value to a virtual machine, depending on its load and status.

Verify that the virtual machine is turned off.

The following user-defined settings affect the memory resource allocation of a virtual machine.

Limit	Places a limit on the consumption of memory for a virtual machine. This value is expressed in megabytes.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in megabytes. If the reservation cannot be met, the virtual machine will not turn on.
Shares	Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the greater share of host memory it receives. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the *vSphere Resource Management* documentation.

You cannot assign a reservation to a virtual machine that is larger than its configured memory. If you give a virtual machine a large reservation and reduce its configured memory size, the reservation is reduced to match the new configured memory size.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand Memory, and allocate the memory capacity for the virtual machine.

Option	Description
Reservation	Guaranteed memory allocation for this virtual machine.
Limit	Upper limit for this virtual machine's memory allocation. Select **Unlimited** to specify no upper limit.
Shares	The values **Low**, **Normal**, **High**, and **Custom** are compared to the sum of all shares of all virtual machines on the server.

3. Click **OK**.

Managing Persistent Memory

ESXi6.7 provides support for the latest computer memory technology, which is called non-volatile memory (NVM) or persistent memory (PMem). PMem combines the high data transfer rate of volatile computer memory with the persistence and resiliency of traditional storage. PMem devices have low access latency and can retain stored data through reboots or power outages.

Modes of Consumption of the Persistent Memory Resources of the Host

When you add a physical PMem device to a host, ESXi detects the PMem resource and exposes it as a host-local PMem datastore to the virtual machines that run on the host. Depending on the guest operating system, virtual machines can have direct access to the PMem resources.

Each host can have only one local PMem datastore that pools and represents all PMem resources of the host.

Persistent memory combines the properties of both memory and storage. So, virtual machines can consume the PMem resources of the ESXi host as memory (through virtual NVDIMM devices) or as storage (through virtual PMem hard disks).

The host-local PMem datastore stores all direct-accessed NVDIMM devices and virtual PMem hard disks.

Virtual PMem (vPMem)

In this mode, if the guest operating system is PMem-aware, the virtual machine can have direct access to the physical PMem resources of the host and use them as standard, byte-addressable memory.

Virtual machines use virtual non-volatile dual in-line memory modules (NVDIMMs) for direct access to PMem. The NVDIMM is a memory device that sits on an ordinary memory channel, but contains non-volatile memory. In vSphere 6.7, the virtual NVDIMM is a new type of device that represents the physical PMem regions of the host. A single virtual machine can have up to 64 virtual NVDIMM devices. Each NVDIMM device is stored on the host-local PMem datastore.

Note: To add an NVDIMM device to a virtual machine, the virtual machine must be of hardware version 14 and the guest operating system must support persistent memory. If the guest operating system is not PMem-aware, you can still use PMem, but you cannot add an NVDIMM device to the virtual machine.

Virtual PMem Disks (vPMemDisk)

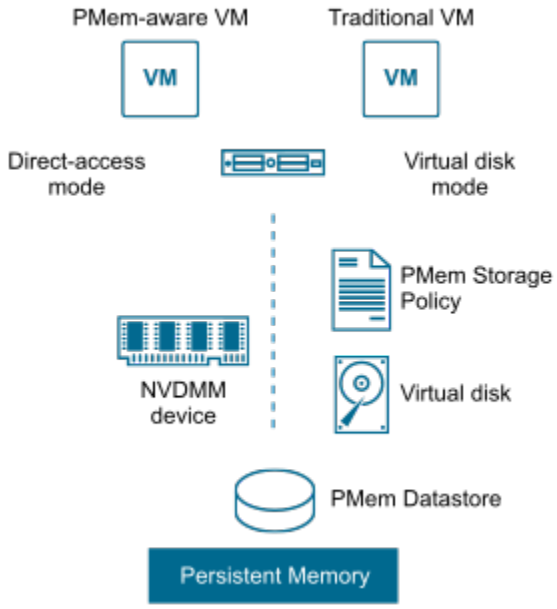
In this mode, the virtual machine does not have direct access to the PMem resources of the host.

You must add a virtual PMem hard disk to the virtual machine. A virtual PMem hard disk is a traditional SCSI disk to which the PMem Storage Policy is applied. The policy automatically places the hard disk on the host-local PMem datastore.

In this mode of usage, there are no requirements for the hardware version of the virtual machine and the guest operating system.

Note: If the guest operating system is not PMem-aware, virtual machines can use PMem only through vPMemDisks.

The following diagram illustrates how the persistent memory components interact.



For information about how to configure and manage VMs with NVDIMMs or virtual persistent memory disks, see the *vSphere Resource Management* documentation.

Add an NVDIMM Device to a Virtual Machine

Add a virtual NVDIMM device to a virtual machine to enable it to use non-volatile, or persistent, computer memory. Non-volatile memory (NVM), or persistent memory (PMem), combines the high data transfer rates of the volatile memory with the persistence and resiliency of traditional storage. The virtual NVDIMM device is a virtual NVM device that can retain stored data through reboots or power source failures.

- Power off the virtual machine.
- Verify that the guest operating system of the virtual machine supports PMem.
- To add an NVDIMM device to a virtual machine, verify that the virtual machine hardware is of version 14 or higher.
- Verify that you have the **Datastore** > **Allocate space** privilege on the virtual machine.
- Verify that the host or the cluster on which the virtual machine resides has available PMem resources.
- To configure vSphere HA for PMem virtual machines:
  - Verify that the virtual machine hardware is of version 19 or higher.
  - Verify that vSphere HA is enabled on the cluster.

If an ESXi host fails or the datastore is no longer accessible, when you add an NVDIMM device to a virtual machine, you can configure vSphere HA to failover all PMem virtual machines on another host.

Note: If a host fails, NVDIMM PMem data cannot be restored. vSphere HA will restart the virtual machine on another host with a new and empty NVDIMM of the same size.

For more information, see the *vSphere Resource Management* guide.

1. Add an NVDIMM device to a virtual machine when you deploy a virtual machine or edit an existing virtual machine.

Option	Action
Create a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine and select **New Virtual Machine**. 2. On the **Select a creation type page**, select **Create a new virtual machine**, and click **Next**. 3. Navigate through the pages of the wizard.

Option	Action
	4. On the **Customize hardware** page, click the **Virtual Hardware** tab. 5. On the **Virtual Hardware** tab, click the **Add New Device** button. 6. From the drop-down menu, select **NVDIMM**.
Edit a virtual machine	1. Right-click a virtual machine in the inventory and select **Edit Settings**. 2. Click the **Virtual Hardware** tab. 3. On the **Virtual Hardware** tab, click the **Add New Device** button. 4. From the drop-down menu, select **NVDIMM**.

The NVDIMM device appears in the Virtual Hardware devices list together with the virtual NVDIMM controller. Each virtual machine can have a maximum of one virtual NVDIMM controller and each NVDIMM controller can have up to 64 virtual NVDIMM devices.

Note: You can change the size of the NVDIMM device at a later time. The virtual machine must be powered off.

2. In the **New NVDIMM** text box, enter the size of the NVDIMM device and select the units from the drop-down menu.

   Note: Adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

3. Expand the **New NVDIMM device** section and select the **Allow failover on another host for all NVDIMM devices** check box.

   Note: When you allow the failover process, if you add another NVDIMM device to the virtual machine, the NVDIMM device will have **PMem HA** enabled. If you want to preserve the NVDIMM content of the virtual machine during a host failure, make sure to deselect the **Allow failover on another host for all NVDIMM devices** check box.

4. If you deploy a virtual machine, click **Next**.
5. If you edit an existing virtual machine, click **OK**.

When you power on the virtual machine, you can view the vSphere HA Protection status of the virtual machine in the **vSphere HA** panel on the **Summary** tab.

Change Memory Hot Add Settings

Memory hot add lets you add memory resources for a virtual machine while that virtual machine is powered on.

- Power off the virtual machine.
- Verify that the virtual machine has a guest operating system that supports memory hot add functionality.
- Verify that the virtual machine compatibility is ESXi 4.x and later.
- Verify that VMware Tools is installed.

Enabling memory hot add produces some memory overhead on the ESXi host for the virtual machine.

Note: If the ESXi host is of version 7.0 Update 2 and earlier, hot-adding memory to a virtual machine with NVIDIA vGPU requires that the ESXi host has a free vGPU slot. Starting with vSphere 7.0 Update 3, the source host does not require to have a free vGPU slot.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Memory**, and select **Enable** to enable adding memory to the virtual machine while it is powered on.
3. Click **OK**.

You can now add memory to a virtual machine, even if the virtual machine is turned on.

Virtual Disk Configuration

You can add large-capacity virtual disks to virtual machines and add more space to existing disks, even when the virtual machine is running. You can set most of the virtual disk parameters during virtual machine creation or after you install the guest operating system.

You can store virtual machine data in a new virtual disk, an existing virtual disk, or a mapped SAN LUN. A virtual disk appears as a single hard disk to the guest operating system. The virtual disk is composed of one or more files on the host file system. You can copy or move virtual disks on the same hosts or between hosts.

For virtual machines running on an ESXi host, you can store virtual machine data directly on a SAN LUN instead of using a virtual disk file. This option is useful if in your virtual machines you run applications that must detect the physical characteristics of the storage device. Mapping a SAN LUN also allows you to use existing SAN commands to manage storage for the disk.

When you map a LUN to a VMFS volume, vCenter Server or the ESXi host creates a raw device mapping (RDM) file that points to the raw LUN. Encapsulating disk information in a file allows vCenter Server or the ESXi host to lock the LUN so that only one virtual machine can write to it. This file has a `.vmdk` extension, but the file contains only disk information that describes the mapping to the LUN on the ESXi system. The actual data is stored on the LUN. You cannot deploy a virtual machine from a template and store its data on a LUN. You can store its data only in a virtual disk file.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

About Virtual Disk Provisioning Policies

When you perform certain virtual machine management operations, you can specify a provisioning policy for the virtual disk file. The operations include creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine.

NFS datastores with Hardware Acceleration and VMFS datastores support the following disk provisioning policies. On NFS datastores that do not support Hardware Acceleration, only thin format is available.

You can use Storage vMotion or cross-host Storage vMotion to transform virtual disks from one format to another.

Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand later on first write from the virtual machine. Virtual machines do not read stale data from the physical device.

Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks. Increasing the size of an Eager Zeroed Thick virtual disk causes a significant stun time for the virtual machine.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed. **Note:** If a virtual disk supports clustering solutions such as Fault Tolerance, do not make the disk thin.

Large Capacity Virtual Disk Conditions and Limitations

Virtual machines with large capacity virtual hard disks, or disks greater than 2 TB, must meet resource and configuration requirements for optimal virtual machine performance.

The maximum value for large capacity hard disks is 62 TB. When you add or configure virtual disks, always leave a small amount of overhead. Some virtual machine tasks can quickly consume large amounts of disk space, which can prevent successful completion of the task if the maximum disk space is assigned to the disk. Such events might include taking snapshots or using linked clones. These operations cannot finish when the maximum amount of disk space is allocated. Also, operations such as snapshot quiesce, cloning, Storage vMotion, or vMotion in environments without shared storage, can take significantly longer to finish.

Virtual machines with large capacity disks have the following conditions and limitations:

- The guest operating system must support large capacity virtual hard disks.
- You can move or clone disks that are greater than 2 TB to ESXi 6.0 or later hosts or to clusters that have such hosts available.
- The datastore format must be one of the following:
  - VMFS5 or later
  - An NFS volume on a Network Attached Storage (NAS) server
  - vSAN
- Fault Tolerance is not supported.
- BusLogic Parallel controllers are not supported.

Change the Virtual Disk Configuration

If you run out of disk space, you can increase the size of the disk. You can change the virtual device node and the persistence mode for virtual disk configuration for a virtual machine.

If you change the disk mode to **Independent - Nonpersistent** or from **Independent - Nonpersistent**, power off the virtual machine.

Verify that you have the following privileges:

- **Virtual machine** > **Configuration** > **Modify device settings** on the virtual machine.
- **Virtual machine** > **Configuration** > **Extend virtual disk** on the virtual machine.
- **Datastore** > **Allocate space** on the datastore.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Hard disk** to view or change the disk settings, and click **OK**.

Option	Description
Maximum Size	Shows the maximum size of this hard disk on this VM. **Note:** Extending the size of a virtual hard disk causes stun time for the virtual machine. The stun time is longer if the virtual disk is of the Eager Zeroed Thick type.
VM storage policy	Select one of the available storage policies. See the *vSphere Storage* documentation for details. **Note:** You cannot change the VM storage policy of an existing PMem hard disk. You also cannot change the storage policy of an existing non-PMem disk to Host-local PMem Default Storage Policy.
Type	Shows the storage type. You cannot change this setting for an existing hard disk. You choose the storage type of a hard disk when you add the hard disk to the virtual machine. For more information about storage types and available disk formats, see the *vSphere Storage* documentation.
Sharing	Specifies sharing information.
Disk File	Lists disk files on the datastore.
Shares	Shares is a value that represents the relative metric for controlling disk bandwidth. The values Low, Normal, High, and Custom are compared to the sum of all shares of all virtual machines on the host.
Limit - IOPs	Allows you to customize IOPs. This value is the upper limit of I/O operations per second allocated to the virtual disk.
Disk mode	Disk mode determines how a virtual disk is affected by snapshots.
Virtual Device Node	Displays the virtual device node.

Use Disk Shares to Prioritize Virtual Machines

You can change the disk resources for a virtual machine. If multiple virtual machines access the same VMFS datastore and the same logical unit number (LUN), use disk shares to prioritize the disk accesses from the virtual machines. Disk shares distinguish high-priority from low-priority virtual machines.

You can allocate the host disk's I/O bandwidth to the virtual hard disks of a virtual machine. Disk I/O is a host-centric resource so you cannot pool it across a cluster.

Shares is a value that represents the relative metric for controlling disk bandwidth to all virtual machines. The values are compared to the sum of all shares of all virtual machines on the server.

Disk shares are relevant only within a given host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.

You can select an IOP limit, which sets an upper bound for storage resources that are allocated to a virtual machine. IOPs are the number of I/O operations per second.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Hard disk** to view the disk options.
3. From the **Shares** drop-down menu, select a value for the shares to allocate to the virtual machine. Alternatively, you can select **Custom** and you can enter a number of shares in the text box manually.
4. In the **Limit - IOPs** box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.
5. Click **OK**.

Determine the Virtual Disk Format and Convert a Virtual Disk from Thin Provision to a Thick Provision Format

When the disk space is exhausted and a thin-provisioned disk cannot expand, the virtual machine cannot boot. If you created a virtual disk in the thin provision format, you can convert it to the thick provision format.

The thin provisioned disk starts small and at first, uses just as much storage space as it needs for its initial operations. After you convert the disk, it grows to its full capacity and occupies the entire datastore space provisioned to it during the disk's creation.

For more information about thin provisioning and available disk formats, see the *vSphere Storage* documentation.

Note: You cannot create thick provisioned disks on NFS datastores. For more information, see the VMware KB article at: https://kb.vmware.com/s/article/2147607.

1. Verify that the disk format of a virtual hard disk is Thin Provision.
   a) Right-click a virtual machine and click **Edit Settings**.
   b) On the **Virtual Hardware** tab, expand **Hard disk** and check the **Type** field.
   c) To exit the wizard, click **Cancel**.
2. To open the datastore management panel, click the **Datastores** tab, and click a datastore from the list.
   The datastore that stores the virtual machine files is listed.
3. Click the **Files** tab, and open the virtual machine folder.
4. Browse to the virtual disk file that you want to convert.
   The file has the `.vmdk` extension.
5. To convert the virtual disk to a thick provision format, select the virtual disk file and click the **Inflate**.
   The **Inflate** window appears.
6. Click **OK**.

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Note: The **Inflate** option might not be available if the virtual disk is thick or when the virtual machine is powered on.

Add a Hard Disk to a Virtual Machine

When you create a virtual machine, a default virtual hard disk is added. You can add another hard disk if you run out of disk space, if you want to add a boot disk, or for other file management purposes. When you add a hard disk to a virtual machine, you can create a virtual disk, add an existing virtual disk, or add a mapped SAN LUN.

You can add a virtual hard disk to a virtual machine before or after you add a SCSI or SATA storage controller. The new disk is assigned to the first available virtual device node on the default controller, for example (0:1). Only device nodes for the default controller are available unless you add additional controllers.

The following ways to add disks can help you plan your disk configuration. These approaches show how you can optimize controller and virtual device nodes for different disks. For storage controller limitations, maximums, and virtual device node behavior, see SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility.

Add an existing hard disk that is configured as a boot disk during virtual machine creation.	To ensure that the virtual machine can boot, remove the existing disk before you add the boot disk. After you add a new hard disk to the virtual machine, you might need to go into the BIOS setup to ensure that the disk you were using to boot the virtual machine is still selected as the boot disk. You can avoid this problem by not mixing adapter types, and by using device node 0 on the first adapter as the boot disk.
Keep the default boot disk and add a new disk during virtual machine creation.	The new disk is assigned to the next available virtual device node, for example (0:1) You can add a new controller and assign the disk to a virtual device node on that controller, for example (1:0) or (1:1).
Add multiple hard disks to an existing virtual machine.	If you add multiple hard disks to a virtual machine, you can assign them to several SCSI or SATA controllers to improve performance. The controller must be available before you can select a virtual device node. For example, if you add controllers 1, 2, and 3, and add four hard disks, you might assign the fourth disk to virtual device node (3:1).

Add a New Hard Disk to a Virtual Machine

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

- Ensure that you are familiar with configuration options and caveats for adding virtual hard disks. See Virtual Disk Configuration.
- Before you add disks greater than 2 TB to a virtual machine, see Large Capacity Virtual Disk Conditions and Limitations.
- Verify that you have the **Virtual machine** > **Configuration** > **Add new disk** privilege on the destination folder or datastore.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add a new hard disk at the end of the creation process.

If you add multiple hard disks to a virtual machine, you can assign them to several controllers to improve performance. For controller and bus node behavior, see SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. Select **Hard Disk** from the drop-down menu.

   The hard disk appears in the Virtual Hardware devices list.

   Note: If the host where the virtual machine resides has available PMem resources, you can place the new hard drive on the host-local PMem datastore.
4. Expand **New hard disk** and customize the settings of the new hard disk.
   a) Enter a size for the hard disk and select the unit from the drop-down menu.
   b) From the **VM storage policy**, select a storage policy or leave the default one.
   c) From the **Location** drop-down menu, select the datastore location where you want to store virtual machine files.
   d) From the **Disk Provisioning** drop-down menu, select the format for the hard disk.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

   e) From the **Shares** drop-down menu, select a value for the shares to allocate to the virtual disk. Alternatively, you can select **Custom** and enter a value in the text box.

      Shares is a value that represents the relative metric for controlling disk bandwidth. The values Low, Normal, High, and Custom are compared to the sum of all shares of all virtual machines on the host.
   f) From the **Limit - IOPs** drop-down menu, customize the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.

      This value is the upper limit of I/O operations per second allocated to the virtual disk.
   g) From the **Disk Mode** drop-down menu, select a disk mode.

Option	Description
Dependent	Dependent disks are included in snapshots.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk even if you revert a snapshot. When you power off or reset a virtual machine, the disk and all its snapshots are preserved.
Independent - Nonpersistent	Disks in nonpersistent mode behave like read-only disks. Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset the virtual machine, or when you delete a snapshot.

h) From the **Virtual Device Node**, select a virtual device node or leave the default one.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine that is using a BusLogic controller with bus sharing turned on.

Related Links

Add an Existing Hard Disk to a Virtual Machine on page 1964

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

Add an RDM Disk to a Virtual Machine on page 1965

You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

Add an Existing Hard Disk to a Virtual Machine

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

- Make sure that you are familiar with controller and virtual device node behavior for different virtual hard disk configurations. See Add a Hard Disk to a Virtual Machine.
- Before you add disks greater than 2 TB to a virtual machine, see Large Capacity Virtual Disk Conditions and Limitations.
- Verify that you have the **Virtual machine** > **Configuration** > **Add existing disk** privilege on the destination folder or datastore.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an existing hard disk at the end of the creation process.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Optional: To delete the existing hard disk, move your pointer over the disk and click the **Remove** icon.

   The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.

3. On the **Virtual Hardware** tab, click the **Add New Device** button.
4. Select **Existing Hard Disk** from the drop-down menu.
   The **Select File** dialog box opens.
5. In the **Select File**, expand a datastore, select a virtual machine folder, and select the disk to add.
6. Click **OK**.
   The disk file appears in the **Contents** column. The **File Type** drop-down menu shows the compatibility file types for this disk.
7. Optional: Expand **New Hard disk** and make further customizations for the hard disk.
8. Click **OK**.

Related Links

Add a New Hard Disk to a Virtual Machine on page 1962

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

Add an RDM Disk to a Virtual Machine on page 1965

You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

Add an RDM Disk to a Virtual Machine

You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

- Ensure that you are familiar with SCSI controller and virtual device node behavior for different virtual hard disk configurations. See Add a Hard Disk to a Virtual Machine.
- Before you add disks greater than 2TB to a virtual machine, see Large Capacity Virtual Disk Conditions and Limitations.
- Required privilege:**Virtual machine** > **Configuration** > **Configure Raw device**

When you give a virtual machine direct access to an RDM disk, you create a mapping file that resides on a VMFS datastore and points to the LUN. Although the mapping file has the same `.vmdk` extension as a regular virtual disk file, the mapping file contains only mapping information. The virtual disk data is stored directly on the LUN.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an RDM disk at the end of the creation process.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button and select **RDM Disk** from the drop-down menu.
   The **Select Target LUN** dialog box opens.
3. In the **Select Target LUN** dialog box, select the target LUN for the raw device mapping and click **OK**.
   The disk appears in the virtual device list.
4. Select the location for the mapping file.
   - To store the mapping file with the virtual machine configuration file, select **Store with the virtual machine**.
   - To select a location for the mapping file, select **Browse** and select the datastore location for the disk.

5. Select a compatibility mode.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, made into a template, or migrated if the migration involves copying the disk.
Virtual	Allows the RDM to behave as if it were a virtual disk, so that you can use such features as taking snapshots, cloning, and so on. When you clone the disk or make a template out of it, the contents of the LUN are copied into a `.vmdk` virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN into a virtual disk.

6. Accept the default or select a different virtual device node.

   In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine using a BusLogic controller with bus sharing turned on.

7. Optional: If you selected virtual compatibility mode, select a disk mode to change the way that disks are affected by snapshots.

   Disk modes are not available for RDM disks using physical compatibility mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk even if you revert a snapshot. When you power off or reset a virtual machine, the disk and all its snapshots are preserved.
Independent - Nonpersistent	Disks in nonpersistent mode behave like read-only disks. Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset the virtual machine, or when you delete a snapshot.

8. Click **OK**.

Related Links

Add a New Hard Disk to a Virtual Machine on page 1962

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

Add an Existing Hard Disk to a Virtual Machine on page 1964

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility

To access virtual disks, CD/DVD-ROM, and SCSI devices, a virtual machine uses storage controllers, which are added by default when you create the virtual machine. You can add controllers or change the controller type after virtual machine creation. You can make these changes while you are in the creation wizard. If you know about node behavior, controller limitations, and compatibility of different types of controllers before you change or add a controller, you can avoid potential boot problems.

How Storage Controller Technology Works

Storage controllers appear to a virtual machine as different types of SCSI controllers, including BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual SCSI. AHCI, SATA, and NVM Express (NVMe) controllers are also available.

NVMe is a standardized protocol designed specifically for high-performance multi-queue communication with NVM devices. ESXi supports the NVMe protocol to connect to local and networked storage devices. For more information, see the *vSphere Storage* documentation.

When you create a virtual machine, the default controller is optimized for best performance. The controller type depends on the guest operating system, the device type, and sometimes, the virtual machine's compatibility. For example, when you create virtual machines with Apple Mac OS X guests and ESXi 5.5 and later compatibility, the default controller type for both the hard disk and the CD/DVD drive is SATA. When you create virtual machines with Windows Vista and later guests, a SCSI controller is the default for the hard disk and a SATA controller is the default for the CD/DVD drive.

In high performance storage environments you can benefit from using VMware Paravirtual SCSI controllers. The VMware Paravirtual SCSI controller ensures greater throughput and lower CPU use, which boosts performance as compared to the other SCSI controller options. For platform support for VMware Paravirtual SCSI controllers, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Each virtual machine can have a maximum of four SCSI controllers and four SATA controllers. The default SCSI or SATA controller is 0. When you create a virtual machine, the default hard disk is assigned to the default controller 0 at bus node (0:0).

When you add storage controllers, they are numbered sequentially 1, 2, and 3. If you add a hard disk, SCSI, or CD/DVD-ROM device to a virtual machine after virtual machine creation, the device is assigned to the first available virtual device node on the default controller, for example (0:1).

If you add a SCSI controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:z), where 1 is SCSI controller 1 and z is a virtual device node from 0 to 15. For SCSI controllers, z cannot be 7. By default, the virtual SCSI controller is assigned to virtual device node (z:7), so that device node is unavailable for hard disks or other devices.

If you add a SATA controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:z), where 1 is SATA controller 1 and z is a virtual device node from 0 to 29. For SATA controllers, you can use device nodes 0 through 29, including 0:7.

Alternatively, each virtual machine can have a maximum of four NVMe controllers. You can reassign an existing or new hard disk or device to that controller. For example, you can assign the hard disk to (x:z), where x is NVMe controller and z is a virtual device node. x has values from 0 to 3, and z has values from 0 to 14.

Storage Controller Limitations

Storage controllers have the following requirements and limitations:

- LSI Logic SAS and VMware Paravirtual SCSI are available for virtual machines with ESXi 4.x and later compatibility.
- AHCI SATA is available only for virtual machines with ESXi 5.5 and later compatibility.
- NVMe is available only for virtual machines with ESXi 6.5 and later compatibility.
- BusLogic Parallel controllers do not support virtual machines with disks larger than 2TB.
- Disks on VMware Paravirtual SCSI controllers might not experience optimal performance if they have snapshots or if the hosts memory is overcommitted.

CAUTION: Changing the controller type after the guest operating system is installed will make the disk and any other devices connected to the adapter inaccessible. Before you change the controller type or add a new controller, make sure that the guest operating system installation media contains the necessary drivers. On Windows guest operating systems, the driver must be installed and configured as the boot driver.

Storage Controller Compatibility

Adding different types of storage controllers to virtual machines that use BIOS firmware can cause operating system boot problems. In the following cases, the virtual machine might fail to boot correctly and you might have to enter the BIOS setup and select the correct boot device:

- If the virtual machine boots from LSI Logic SAS or VMware Paravirtual SCSI, and you add a disk that uses BusLogic, LSI Logic, or AHCI SATA controllers.
- If the virtual machine boots from AHCI SATA, and you add BusLogic Parallel or LSI Logic controllers.

Adding additional disks to virtual machines that use EFI firmware does not cause boot problems.

Table 160: VMware Storage Controller Compatibility

Existing Controller	Added Controller						
	BusLogic Parallel	**LSI Logic**	**LSI Logic SAS**	**VMware Paravirtual SCSI**	**AHCI SATA**	**IDE**	**NVMe**
BusLogic Parallel	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic SAS	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes	Usually Works
VMware Paravirtual SCSI	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes	Usually Works
AHCI SATA	Requires BIOS setup	Requires BIOS setup	Yes	Yes	Yes	Yes	Yes
IDE	Yes	Yes	Yes	Yes	Yes	N/A	Yes
NVMe	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes	Usually Works

Add a SATA Controller

If a virtual machine has multiple hard disks or CD/DVD-ROM devices, you can add up to three additional SATA controllers to assign the devices to. When you spread the devices among several controllers, you can improve performance and avoid data traffic congestion. You can also add additional controllers if you exceed the thirty-device limit for a single controller.

- Verify that the virtual machine compatibility is ESXi 5.5 and later.
- Verify that you are familiar with storage controller behavior and limitations. See SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility.
- Verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.

You can boot virtual machines from SATA controllers and use them for large-capacity virtual hard disks.

Not all guest operating systems support AHCI SATA controllers. Typically, when you create virtual machines with ESXi 5.5 and later compatibility and Mac OS X guest operating systems, a SATA controller is added by default for the virtual hard disk and CD/DVD-ROM devices. Most guest operating systems, including Windows Vista and later have a default SATA

controller for CD/DVD-ROM devices. To verify support, see the *VMware Compatibility Guides* at http://www.vmware.com/resources/compatibility.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. Select **SATA Controller** from the drop-down menu.
   The controller appears in the Virtual Hardware devices list.
4. Click **OK**.

You can add a hard disk or CD/DVD drive to the virtual machine and assign it to the new controller.

Add a SCSI Controller to a Virtual Machine

Many virtual machines have a SCSI controller by default, depending on the guest operating system. If you have a heavily loaded virtual machine with multiple hard disks, you can add up to three additional SCSI controllers to assign the disks to. When you spread the disks among several controllers, you can improve performance and avoid data traffic congestion. You can also add additional controllers if you exceed the 15-device limit for a single controller.

Verify that you have the**Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button. add a new SCSI controller.
3. Select **SCSI Controller** from the drop-down menu.
   The controller appears in the Virtual Hardware device list.
4. Click **OK**.

You can now add a hard disk or other SCSI device to the virtual machine and assign it to the new SCSI controller.

Add a Paravirtualized SCSI Adapter

You can add a VMware Paravirtual SCSI high performance storage controller to a virtual machine to provide greater throughput and lower CPU use.

- Verify that the virtual machine has a guest operating system with VMware Tools installed.
- Verify that the virtual machine compatibility is ESXi 4.x and later.
- Ensure that you are familiar with the VMware Paravirtual SCSI controller type.
- To access boot disk devices attached to a VMware Paravirtual SCSI controller, verify that the virtual machine has a Windows 2003 or Windows 2008 guest operating system.
- In some operating systems, before you change the controller type, create a virtual machine with an LSI Logic controller, install VMware Tools, and then change to paravirtual mode.

VMware Paravirtual SCSI controllers are best suited for environments, especially SAN environments, running I/O-intensive applications.

For information about SCSI controller maximums and virtual device assignments, see SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. Select **SCSI Controller** from the drop-down menu.
4. Expand **New SCSI controller** and from the **Change Type** menu, select **VMware Paravirtual**.
   The controller appears at the bottom of the Virtual Hardware device list.

5. Click **OK**.

Add an NVMe Controller

If a virtual machine has multiple hard disks, you can add up to four virtual NVMe controllers to which to assign the virtual disks. Using an NVMe controller significantly reduces the software overhead for processing guest OS I/O, as compared to AHCI SATA or SCSI controllers.

- Verify that the virtual machine has a guest operating system that supports NVMe.
- Verify that the virtual machine compatibility is ESXi 6.5 or later.
- Verify that you are familiar with storage controller behaviour and limitations. See SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility.
- Verify that you have the **Virtual machine** > **Configuration** > **Add new disk** privilege on the virtual machine.

NVMe controllers perform best with virtual disks on an all-flash disk array, local NVMe SSD, and PMem storage.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. Select **NVMe Controller** from the drop-down menu.

   The controller appears in the Virtual Hardware devices list.
4. Click **OK**.

You can add a hard disk to the virtual machine and assign it to the NVMe controller.

Change the SCSI Controller Configuration

You can specify the SCSI controller type and you can set the type of SCSI bus sharing for a virtual machine.

- Verify that you are familiar with the limitations and conditions for configuring SCSI controllers. See SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility.
- Verify that you have the **Virtual machine** > **Configuration** > **Modify device settings** privilege on the virtual machine.

The choice of a SCSI controller type does not affect whether your virtual disk is an IDE or SCSI disk. The IDE adapter is always ATAPI. The default for your guest operating system is already selected.

The choice of a SCSI bus sharing option determines whether virtual machines on different hosts can access the same virtual disk.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **SCSI controller**, and select a SCSI controller type from the **Change Type** drop-down menu.

   CAUTION: Changing the SCSI controller type might result in a virtual machine boot failure.

   Do not select a BusLogic Parallel controller for virtual machines with disks larger than 2 TB. This controller does not support large capacity hard disks.

   The vSphere Client displays information about what happens if you change the SCSI controller type. If you select a controller type that is not recommended for the virtual machine's guest operating system, a warning is displayed.
3. Expand **SCSI controller** and select the type of sharing in the **SCSI Bus Sharing** drop-down menu.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.
Physical	Virtual disks can be shared by virtual machines on any ESXi host.

Option	Description
Virtual	Virtual disks can be shared by virtual machines on the same ESXi host.

For virtual or physical bus sharing, select **Thick provision eager zeroed** when you create the disk.

4. Click **OK**.

Virtual Machine Network Configuration

vSphere networking features provide communication between virtual machines on the same host, between virtual machines on different hosts, and between other virtual and physical machines. When you configure networking for a virtual machine, you select or change an adapter type, a network connection, and whether to connect the network when the virtual machine powers on.

Network Adapter Basics

When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.

Network Adapter Types

The type of network adapters that are available depend on the following factors:

- The virtual machine compatibility, which depends on the host that created or most recently updated it.
- Whether the virtual machine compatibility has been updated to the latest version for the current host.
- The guest operating system.

Supported NICs currently differ between an on-premises environment and VMware Cloud on AWS. The following NIC types are supported in an on-premises deployment:

E1000E	Emulated version of the Intel 82574 Gigabit Ethernet NIC. E1000E is the default adapter for Windows 8 and Windows Server 2012.
E1000	Emulated version of the Intel 82545EM Gigabit Ethernet NIC, with drivers available in most newer guest operating systems, including Windows XP and later and Linux versions 2.4.19 and later.
Flexible	Identifies itself as a Vlance adapter when a virtual machine boots, but initializes itself and functions as either a Vlance or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlance adapter to the higher performance VMXNET adapter.
Vlance	Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in 32-bit legacy guest operating systems. A virtual machine configured with this network adapter can use its network immediately.
VMXNET	Optimized for performance in a virtual machine and has no physical counterpart. Because operating system vendors do not provide built-in drivers for this card, you must install VMware Tools to have a driver for the VMXNET network adapter available.
VMXNET 2 (Enhanced)	Based on the VMXNET adapter but provides high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads. VMXNET 2 (Enhanced) is available only for some guest operating systems on ESX/ ESXi 3.5 and later.
VMXNET 3	A paravirtualized NIC designed for performance. VMXNET 3 offers all the features available in VMXNET 2 and adds several new

	features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2.
PVRDMA	A paravirtualized NIC that supports remote direct memory access (RDMA) between virtual machines through the OFED verbs API. All virtual machines must have a PVRDMA device and should be connected to a distributed switch. PVRDMA supports VMware vSphere vMotion and snapshot technology. It is available in virtual machines with hardware version 13 and guest operating system Linux kernel 4.6 and later. For information about assigning an PVRDMA network adapter to a virtual machine, see the *vSphere Networking* documentation.
SR-IOV passthrough	Representation of a virtual function (VF) on a physical NIC with SR-IOV support. The virtual machine and the physical adapter exchange data without using the VMkernel as an intermediary. This adapter type is suitable for virtual machines where latency might cause failure or that require more CPU resources. SR-IOV passthrough is available in ESXi 6.0 and later for guest operating systems Red Hat Enterprise Linux 6 and later, and Windows Server 2008 R2 with SP2. An operating system release might contain a default VF driver for certain NICs, while for others you must download and install it from a location provided by the vendor of the NIC or of the host. For information about assigning an SR-IOV passthrough network adapter to a virtual machine, see the *vSphere Networking* documentation.

For network adapter compatibility considerations, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Legacy Network Adapters and ESXi Virtual Hardware Versions

The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to use a virtual hardware version, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Network Adapters and Legacy Virtual Machines

Legacy virtual machines are virtual machines that are supported by the product in use, but are not current for that product. The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to correspond with an upgrade to a newer version of an ESXi host, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Change the Virtual Machine Network Adapter Configuration

You can change the virtual machine network configuration, including its power-on behavior and resource allocation.

For details about configuring the networking for virtual machine network adapters, see the *vSphere Networking* documentation.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Optional: Change the **Status** settings.

Option	Description
Connected	Select or deselect this option while the virtual machine is running to connect or disconnect the virtual network adapter. This check box is not available when the virtual machine is turned off.
Connect at power on	Select this option for the virtual network adapter to connect to the network when the virtual machine turns on. If you do not check this option, you must manually connect the adapter in order for the virtual machine to access the network.

3. If the network adapter is connected to a distributed port group of a distributed switch that has vSphere Network I/O Control version 3 enabled, allocate bandwidth to the adapter.

   Note: You cannot allocate bandwidth to **SR-IOV passthrough** network adapters.

   a) From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.
   b) In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.
   c) In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.
4. Click **OK**.

Add a Network Adapter to a Virtual Machine

You can add a network adapter (NIC) to a virtual machine to connect to a network, to enhance communications, or to replace an older adapter. When you add a NIC to a virtual machine, you select the adapter type, network connection, whether the device should connect when the virtual machine is turned on, and the bandwidth allocation.

For details about configuring the networking for virtual machine network adapters, see the *vSphere Networking* documentation

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button and select **Network Adapter** from the drop-down menu.

   The new network adapter appears at the bottom of the device list.
3. Expand **New Network** and select the standard or distributed port group to connect to.

   The menu lists all standard and distributed port groups that are available for virtual machine use on the host.

   If you want to provision bandwidth to the network adapter from a reserved quota by using vSphere Network I/O Control version 3, select a port group that is associated with the network resource pool that provides the quota.

4. Optional: Review and optionally change the **Status** settings.

Option	Description
Connected	Select this option while the virtual machine is running to connect or disconnect the virtual network adapter. This check box is not available when the virtual machine is turned off.
Connect at power on	Select this option for the virtual network adapter to connect to the network when the virtual machine turns on. If you do not check this option, you must manually connect the adapter for the virtual machine to access the network.

5. Deactivate DirectPath I/O if that seems appropriate in your environment.

   DirectPath I/O allows virtual machine access to physical PCI functions on platforms with an I/O Memory Management Unit. Some features become unavailable with DirectPath I/O enabled, others become available. See the *vSphere Networking* documentation for details.

6. If the network adapter is connected to a distributed port group of a distributed switch that has vSphere Network I/O Control version 3 enabled, allocate bandwidth to the adapter.

   Note: You cannot allocate bandwidth to **SR-IOV passthrough** network adapters.

   a) From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.
   b) In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.
   c) In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.

7. Click **OK**.

Parallel and Serial Port Configuration

Parallel and serial ports are interfaces for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port or to a file on the host computer. You can also use it to establish a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. You can add parallel and serial ports and change the parallel and serial port configuration. Hardware version 11 and later versions allow you to configure virtual machines in such a way that serial and parallel ports are absent from the virtual chipset altogether.

Starting with vSphere 7.0, you cannot add, remove, and configure parallel ports. For information, see https://kb.vmware.com/s/article/78978.

Using Serial Ports with vSphere Virtual Machines

You can set up virtual serial port connections for vSphere virtual machines in several ways. The connection method that you select depends on the task that you need to accomplish.

You can set up virtual serial ports to send data in the following ways.

Physical serial port on the host	Sets the virtual machine to use a physical serial port on the host computer. This method lets you use an external modem or a hand-held device in a virtual machine.
Output to file	Sends output from the virtual serial port to a file on the host computer. This method lets you capture the data that a program running in the virtual machine sends to the virtual serial port.
Connect to a named pipe	Sets a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. With this method, two virtual machines or a virtual machine and a process on the host can communicate as if they

	were physical machines connected by a serial cable. For example, use this option for remote debugging of a virtual machine.
Connect over the network	Enables a serial connection to and from a virtual machine's serial port over the network. The Virtual Serial Port Concentrator (vSPC) aggregates traffic from multiple serial ports onto one management console. vSPC behavior is similar to physical serial port concentrators. Using a vSPC also allows network connections to a virtual machine's serial ports to migrate seamlessly when you use vMotion to migrate the virtual machine. For requirements and steps to configure the Avocent ACS v6000 virtual serial port concentrator, see http://kb.vmware.com/kb/1022303.

Server and Client Connections for Named Pipe and Network Serial Ports

You can select a client or server connection for serial ports. Your selection determines whether the system waits for a connection or initiates it. Typically, to control a virtual machine over a serial port, you select a server connection. This selection lets you control the connections, which is useful if you connect to the virtual machine only occasionally. To use a serial port for logging, select a client connection. This selection lets the virtual machine connect to the logging server when the virtual machine starts and to disconnect when it stops.

Supported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, serial ports that are integrated into the motherboard are supported. A virtual machine can use up to 32 serial ports.

Unsupported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, the serial ports connected through USB are not supported for serial port passthrough. They might be supported by USB passthrough from an ESXi host to a virtual machine. See USB Configuration from an ESXi Host to a Virtual Machine.

In addition, you cannot use Migration with VMotion when you use a physical serial port for serial passthrough.

Adding a Firewall Rule Set for Serial Port Network Connections

If you add or configure a serial port that is backed by a remote network connection, ESXi firewall settings can prevent transmissions.

Before you connect network-backed virtual serial ports, you must add one of the following firewall rule sets to prevent the firewall from blocking communication:

- **VM serial port connected to vSPC**. Use to connect the serial port output through a network with the **Use virtual serial port concentrator** option enabled to allow only outgoing communication from the host.
- **VM serial port connected over network**. Use to connect the serial port output through a network without the virtual serial port concentrator.

Important: Do not change the allowed IP list for either rule set. Updates to the IP list can affect other network services that might be blocked by the firewall.

For details about allowing access to an ESXi service through the firewall, see the *vSphere Security* documentation.

Configure Virtual Machine Communication Interface Firewall

You can configure the virtual machine Communication Interface firewall (VMCI) to restrict virtual machines accessing the hypervisor-based services and VMCI-based services.

You can restrict VMCI usage to a subset of VMCI-based services on each virtual machine. For example, you can allow certain virtual machines to access VMCI services and deny access to others for security reasons.

Currently, VMCI devices support guest to host communication. A virtual machine can communicate with VMCI services through the following means:

- ESXi hypervisor
- Services installed on the host operating system in the form of a vmkernel module
- Applications installed by a verified vSphere Installation Bundle

Change the Serial Port Configuration

You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network. You can add up to 32 serial ports to a virtual machine.

- Check that you know the correct media types for the port to access, vSPC connections, and any conditions that might apply. See Using Serial Ports with vSphere Virtual Machines.
- To connect a serial port over a network, add a Firewall rule set. See Adding a Firewall Rule Set for Serial Port Network Connections.
- To use authentication parameters with network serial port connections, see Authentication Parameters for Virtual Serial Port Network Connections.
- Required privileges:
  - **Virtual machine** > **Configuration** > **Modify device settings** on the virtual machine.
  - **Virtual machine** > **Interaction** > **Device connection** on the virtual machine to change the device connection status.

Virtual machines can be in a powered-on state during configuration.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Serial port**, and select a connection type.

Option	Action
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.
Use named pipe	Select this option to set a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. 1. Type a name for the pipe in the **Pipe Name** field. 2. Select the **Near end** and **Far end** of the pipe from the drop-down menus.
Use Network	Select **Use network** to connect through a remote network. 1. Select the network backing. – Select **Server** to have the virtual machine monitor incoming connections from other hosts. – Select **Client** to have the virtual machine initiate a connection to another host.

Option	Action
	2. Enter a **Port URI**. The URI is the remote end of the serial port to which the virtual machine's serial port should connect. 3. If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select **Use Virtual Serial Port Concentrator** and enter the vSPC URI location.
Printer	Select **Printer** to connect to a remote printer.

3. Optional: Select **Yield CPU on poll**.

   Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.

4. Optional: Select **Connect at power on** to connect the serial port when the virtual machine powers on.

5. Click **OK**.

Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Authentication Parameters for Virtual Serial Port Network Connections

When you establish serial port connections over the network, you can use authentication parameters to secure the network. These parameters can support an encrypted connection with a remote system using SSL over Telnet or Telnets, or an encrypted connection with a concentrator using SSL over Telnet or Telnets.

URI Forms

If you do not use virtual serial port network connection (vSPC) and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system. You use one of the following formats:

- Telnet over TCP.

  ```
  telnet://host:port
  ```

  The virtual machine and remote system can negotiate and use SSL if the remote system supports the Telnet authentication option. If not, the connection uses unencrypted text (plain text).
- Telnets over SSL over TCP.

  ```
  telnets://host:port
  ```

  SSL negotiation begins immediately, and you cannot use the Telnet authentication option.

Authentication Parameters

For an encrypted connection, the URI includes a set of authentication parameters. Enter the parameters as key words or key/value pairs. You can enter authentication parameters for secure Telnet (`telnets`), or for Telnet (`telnet`) as shown in the following syntax:

```
telnet://host:port#key[=value] [&key[=value] ...]
```

The first parameter must have a number sign (#) prefix. Additional parameters must have an ampersand (&) prefix. The following parameters are supported.

thumbprint=*value*

Specifies a certificate thumbprint against which the peer certificate thumbprint is compared. When you specify a thumbprint, certificate verification is enabled.

peerName=*value*

Specifies the peer name that is used to validate the peer certificate. When you specify a peer name, certificate verification is enabled.

verify

Forces certificate verification. The virtual machine will verify that the peer certificate subject matches the specified peerName and that it was signed by a certificate authority known to the ESXi host. Verification is enabled if you specify a thumbprint or peerName

cipherList=*value*

Specifies a list of SSL ciphers. The ciphers are specified as a list separated by colons, spaces, or commas.

Establishing Serial Port Network Connections to a Client or Server

Simple Server Connection	To connect to a virtual machine's serial port from a Linux or Windows operating system if you do not use vSPC, configure the virtual machine with a serial port connected as a server with a `telnet://:12345` URI. To access a virtual serial port from a client, use `telnet` *`yourESXiServerIPAddress`* `12345`.
Secure Server Connection	To enforce an encrypted connection to the virtual machine's serial port from a Linux operating system, you can configure Telnet to enforce encryption by configuring the virtual machine with a serial port connected as a server with a `telnet://:12345#verify` URI. To access a virtual serial port from a client, use `telnet-ssl` *`yourESXServerName`* `12345`. This connection will fail if the Telnet program you are using does not support SSL encryption.
Simple Client Connection	If you are running a Telnet server on your system and you want the virtual machine to automatically connect to it, you can configure the virtual machine as a client using `telnet://`*`yourLinuxBox`*`:23`. The Virtual machine keeps initiating the Telnet connection to port 23 on *`yourLinuxBox`*.
Secure Client Connection	Additional URI options allow you to enforce a specific server certificate and restrict the ciphers being used. Virtual machines with a serial port configured as a client with `telnet://`*`ipOfYourLinuxBox`*`:23#cipherList=DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA&peerName=`*`myLinuxBoxName.withDomain`* will connect to *`ipOfYourLinuxBox`* only if the system supports one of two listed ciphers, and if it presents a trusted certificate issued to *`myLinuxBoxName.withDomain`*. Replace *`.withDomain`* with the full domain name, for example, `example.org`.

Add a Serial Port to a Virtual Machine

You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network. A virtual machine can use up to 32 serial ports.

- Verify that the virtual machine is powered off.
- Check that you know the correct media types for the port to access, vSPC connections, and any conditions that might apply. See Using Serial Ports with vSphere Virtual Machines.
- To connect a serial port over a network, add a Firewall rule set. See Adding a Firewall Rule Set for Serial Port Network Connections.
- To use authentication parameter with network serial port connections, see Authentication Parameters for Virtual Serial Port Network Connections.
- Required privilege: **Virtual Machine** > **Configuration** > **Add or Remove Device**

Important: With virtual hardware version 11 and later, if you configure a virtual machine without serial ports, they are entirely removed from the virtual chipset and they are not visible to the virtual machine OS.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. Select **Serial Port** from the drop-down menu.

   The new serial port appears at the bottom of the device list.
4. From the **New Serial port** drop-down menu, select a connection type.

Option	Action
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. To select an output file to connect to the serial port, click **Browse** .
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use named pipe	Select this option to set a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. 1. Enter a name for the pipe in the **Pipe Name** field. 2. Select the **Near end** and **Far end** of the pipe from the drop-down menus.
Use Network	To connect through a remote network, select **Use network**. 1. Select the network backing. – To have the virtual machine monitor incoming connections from other hosts, select **Server**. – To have the virtual machine initiate a connection to another host, select **Client**. 2. Enter a **Port URI**. The URI is the remote end of the serial port to which the virtual machine's serial port should connect. 3. If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select **Use Virtual Serial Port Concentrator** and enter the **vSPC URI** location.

5. Optional: Select **Yield CPU on poll**.

   Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.

6. Click **OK**.

Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Other Virtual Machine Device Configuration

In addition to configuring virtual machine CPU and memory, and adding a hard disk and virtual NICs, you can also add and configure virtual hardware, such as DVD/CD-ROM drives. Not all devices are available to add and configure. For example, you cannot add a video card, but you can configure available video cards and PCI devices.

For information how to add, remove, and configure floppy drives or SCSI devices, see https://kb.vmware.com/s/article/78978.

Change the CD/DVD Drive Configuration

You can configure DVD or CD devices to connect to client devices, host devices, datastore ISO files, or content library ISO files.

Configure a Datastore ISO File for the CD/DVD Drive

To install a guest operating system and its applications on a new virtual machine, you can connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host.

Verify that you have the following privileges:

- **Virtual machine** > **Interaction** > **Configure CD media** on the virtual machine.
- **Datastore** > **Browse datastore** on the datastore to which you upload the installation media ISO image.
- **Datastore** > **Low level file operations** on the datastore to which you upload the installation media ISO image.

If an ISO image is not available on a local or shared datastore, upload the file to a datastore from your local system by using the datastore file browser. See Upload ISO Image Installation Media for a Guest Operating System.

To avoid performance issues and possible conflicts between virtual machines that might try to simultaneously access the ISO image, unmount and disconnect the ISO file when the installation finishes.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Expand **CD/DVD drive**, and select **Datastore ISO File** from the drop-down menu.

   The **Select File** dialog box opens

3. Browse to select the file and click **OK**.
4. From the **Virtual Device Node** drop-down menu, select the node that the drive uses in the virtual machine.
5. Optional: Select **Connect At Power On** to connect the device when the virtual machine powers on.
6. Click **OK**.
7. Power on the virtual machine and click the **Summary** tab.
8. Expand the **VM Hardware** panel and click the **Connected** icon next to the datastore ISO file to connect the device

Configure a Content Library ISO File for the CD/DVD Drive

To install a guest operating system and its applications on a new virtual machine, you can connect the CD/DVD device to an ISO file that is stored in a content library.

Verify that you have the **Virtual machine** > **Interaction** > **Configure CD media** privilege on the virtual machine.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Expand **CD/DVD drive** and select **Content Library ISO File** from the drop-down menu.
   The **Choose an ISO image to mount dialog** box opens.
3. Select the ISO file and click **OK**.
4. Optional: Select **Connect At Power On** to connect the device when the virtual machine powers on.
5. Click **OK**.
6. Power on the virtual machine and click the **Summary tab**.
7. Expand the **VM Hardware** panel and from the drop-down menu next to the **Connected** icon, select to connect the CD/DVD drive to a content library ISO file.

Configure a Host Device Type for the CD/DVD Drive

You can configure the CD/DVD drive of a virtual machine to connect to a physical CD or DVD device on the host so that you can install a guest operating system, VMware Tools, or other applications.

- Verify that the virtual machine is powered off.
- You cannot use vMotion to migrate virtual machines that have CD drives that are backed by the physical CD drive on the host. Disconnect these devices before you migrate the virtual machine.
- Verify that you have the **Virtual machine** > **Interaction** > **Configure CD media** privilege on the virtual machine.

When you create a virtual machine, a controller is added by default and the CD/DVD drive is attached to that controller. The controller and driver type depend on the guest operating system. Typically, virtual machines with newer guest operating systems have a SATA controller and CD/DVD drive. Other guests use an IDE controller and CD/DVD drive.

If you connect to media that does not require you to power off the virtual machine, you can select the media to connect to from the CD/DVD drive connection icon on the virtual machine **Summary** tab.

When you add a CD/DVD drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device.

For information how to add, remove, and configure SCSI devices, see https://kb.vmware.com/s/article/78978.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CD/DVD** and select **Host Device** from the drop-down menu.
3. Optional: Select **Connect At Power On** to connect the device when the virtual machine powers on.
4. If more than one type of CD/DVD media is available on the host, select the media.
5. In the **Virtual Device Node** drop-down menu, select the node the drive uses in the virtual machine.
   The first available node is selected by default. You do not typically need to change the default.
6. Click **OK**.
7. Power on the virtual machine and click the **Summary** tab.

The connected CD/DVD device appears in the **VM Hardware** list.

Configure a Client Device Type for the CD/DVD Drive

To install a guest operating system and its applications or other media on a virtual machine, you can connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Client.

Verify that the virtual machine is turned on.

By default, passthrough IDE mode is used for remote client device access. You can write or burn a remote CD only through passthrough mode access.

1. Navigate to a virtual machine in the inventory and click the **Summary** tab.
2. In the **VM Hardware** panel, click the **CD/DVD drive** connection icon, select an available drive to connect to, and browse for the CD/DVD media.
   An Access Control dialog box opens. Click **allow** to proceed. To change your selection, click the connection icon, select **Disconnect**, and select a different option.

How do I Add or Modify a Virtual Machine CD or DVD Drive

CD/DVD drives are necessary for installing a guest operating system and VMware Tools.

- Verify that the virtual machine is powered off.
- If an ISO image file is not available on a local or shared datastore, upload an ISO image to a datastore from your local system by using the datastore file browser. See Upload ISO Image Installation Media for a Guest Operating System.
- Verify that you have the**Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.

When you power on the virtual machine, you can select the media to connect to from the **VM Hardware** panel on the virtual machine **Summary** tab.

The following conditions exist.

- If you add a CD/DVD drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device.

- You must disconnect virtual machines that have CD drives that are backed by the physical CD drive on the host, before you migrate the virtual machine.
- You access the host CD-ROM device through emulation mode. Passthrough mode is not functional for local host CD-ROM access. You can write or burn a remote CD only through passthrough mode access, but in emulation mode you can only read a CD-ROM from a host CD-ROM device.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Select your task.

Option	Description
Add a CD/DVD drive	On the **Virtual Hardware** tab, click the **Add New Device** button and select **CD/DVD Drive**.
Modify CD/DVD settings	On the **Virtual Hardware** tab, expand **CD/DVD drive** and change the configuration settings.

3. To change CD/DVD settings, select the device type from the **CD/DVD drive** drop-down menu.

Option	Action
Client Device	Select this option to connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Client. From the **Device Mode** drop-down menu, select **Passthrough CD-ROM**.
Host Device	1. Select to connect the CD/DVD device to a physical DVD or CD device on the host. 2. From the **CD/DVD Media** drop-down menu, select the media to connect to. 3. From the **Device Mode** drop-down menu, select **Emulate CD-ROM**.
Datastore ISO File	Select this option to connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host. The **Select File** dialog box opens. 1. In the **Select File** dialog box, browse to the file containing the ISO image to connect to. 2. Click **OK**.
Content Library ISO File	Select this option to connect the CD/DVD device to an ISO file that is stored in a content library. The **Choose an ISO image to mount** dialog box opens 1. In the **Choose an ISO image to mount**, select the ISO image to connect to. 2. Click **OK**.

4. Optional: Specify additional settings for the CD/DVD drive.

Option	Description
Connect At Power On	Select this option to connect to the device when the virtual machine turns on.
Device Mode	Select **Passthrough CD-ROM** for a CD/DVD drive that is connected to the physical client machine. Select **Emulate CD-ROM** otherwise.
Virtual Device Node	Specify the location of the ISO that you are mounting. To change the device node from the default, select a new mode from the **Virtual Device Node** drop-down menu. For example, if you select SATA(0:2), the guest operating system detects the drive as ID 2 on controller 0.

5. Power on the virtual machine and click the **Summary** tab.
6. Expand the **VM Hardware** panel and click **Connected** next to select to.

You can now install the guest operating system or other applications.

Add a PCI Device to a Virtual Machine

Starting with vSphere 7.0, virtual machines can specify PCI passthrough devices by their vendor and model names. vSphere Distributed Resource Scheduler (DRS) uses these names to identify the hosts containing all specified devices available for passthrough. vSphere DRS can also recognize whether a PCI device is used by another virtual machine, and assign only the available devices to the virtual machine when it powers on.

Verify that you have the privileges that you need for the task that you plan to perform.

- If you plan to add a PCI device when you edit a virtual machine, verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege.
- If you plan to increase the memory reservation when you edit a virtual machine, verify that you have the **Virtual machine** > **Configuration** > **Change resource** privilege.
- If you plan to reduce the virtual machine memory when you edit a virtual machine, verify that you have the **Virtual machine** > **Configuration** > **Change Memory** privilege.
- Power off the virtual machine.
- To use Dynamic DirectPath I/O, verify that the virtual machine is compatible with ESXi 7.0 or later.
- To use DirectPath, verify that Intel Virtualization Technology for Directed I/O (VT-d) or AMD I/O Virtualization Technology (IOMMU) is enabled in the host BIOS.
- Verify that the PCI devices are connected to the host and marked as available for passthrough. If your ESXi host is configured to boot from a USB device, or if the active coredump partition is configured to be on a USB device or SD cards connected through USB channels, deactivate the USB controller for passthrough. VMware does not support USB controller passthrough for hosts that boot from USB devices or SD cards connected through USB channels. A configuration in which the active coredump partition is configured to be on a USB device or SD card connected through USB channels is also not supported. For information, see http://kb.vmware.com/kb/1021345.
- To use NVIDIA GRID vGPU graphic devices:
  - Verify that an NVIDIA GRID vGPU graphic device with an appropriate driver is installed on the host. See the *VMware ESXi Upgrade* documentation.
  - Verify that the virtual machine is compatible with 6.0 and later.
- To add multiple NVIDIA GRID vGPUs to a virtual machine:
  - Verify that the virtual machine is compatible with ESXi 6.7 Update 2 and later.
  - Use only NVIDIA vGPU profiles with a maximum frame buffer.
  - Only Q-series and C-series vGPU types are supported.

You can connect to the guest operating system of a virtual machine all PCI devices that are configured on an ESXi host and made available for passthrough.

PCI vSphere DirectPath I/O devices

vSphere DirectPath I/O allows a virtual machine to specify and access directly the physical PCI and PCIe devices connected to a specific host. This way you can directly access devices, such as high-performance graphics or sound cards. You can connect each virtual machine to up to sixteen PCI devices.

You configure PCI devices on an ESXi host to make them available for passthrough to a virtual machine. See the *vSphere Networking* documentation. However, you must not enable PCI passthrough for ESXi hosts that are configured to boot from USB devices.

When PCI vSphere DirectPath I/O devices are made available to a virtual machine, you cannot perform certain operations on the virtual machine. These operations include suspending, migration with vMotion, and taking or restoring snapshots of the virtual machine.

PCI vSphere Dynamic DirectPath I/O devices	vSphere Dynamic DirectPath I/O provides you with the ability to assign multiple PCI passthrough devices to a virtual machine. vSphere Dynamic DirectPath I/O allows vSphere DRS to identify a host within the cluster that has an available device with the same vendor and model name. **Note:** When you add a PCI device to a virtual machine, the full memory size of the virtual machine is automatically reserved.
NVIDIA GRID GPU devices	If an host has an NVIDIA GRID GPU graphics device, you can configure a virtual machine to use the NVIDIA GRID virtual GPU (vGPU) technology. NVIDIA GRID vGPU devices optimize complex graphics operations and make them run at high performance without overloading the CPU. NVIDIA GRID vGPU provides unparalleled graphics performance and scalability by sharing a single physical GPU among multiple virtual machines as separate vGPU-enabled passthrough devices. Starting with vSphere 7.0 Update 2, you can configure a virtual machine to use the NVIDIA Multi-Instance GPU (MIG) feature. By using NVIDIA MIG, you can securely partition applicable GPUs into separate GPU instances. Each GPU instance has dedicated resources, such as memory, memory caches, and compute cores. If a GPU is in MIG mode, you can assign unique vGPU profile names to a virtual machine. VMware will create GPU and compute instances automatically, so you should not create them manually.

1. Add a PCI device to a virtual machine when you deploy a virtual machine or edit an existing virtual machine.

Option	Action
Create a new virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine and select **New Virtual Machine**. 2. On the **Select a creation type** page, select **Create a new virtual machine**, and click **Next**. 3. Navigate through the pages of the wizard. 4. On the **Customize hardware** page, click the **Virtual Hardware** tab.
Edit a virtual machine	1. Right-click a virtual machine in the inventory and select **Edit Settings**. 2. Click the **Virtual Hardware** tab.

2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. From the drop-down menu, under **Other Devices**, select **PCI Device**.
4. Expand the **New PCI device** section and select the access type.

Option	Action
DirectPath IO	From the **PCI Device** drop-down menu, select the PCI device to connect to the virtual machine.
Dynamic DirectPath IO	From the **PCI Device** drop-down menu, expand **Select Hardware** and select the PCI passthrough devices by their vendor, model name, and hardware label in brackets, if present. **Note:** The hardware label allows you to restrict the virtual machine placement to specific hardware instances. When the first PCI device that you select is with a specific hardware label, all other PCI devices that you want to add must have the same

Option	Action
	hardware label. If the first PCI device is with an empty hardware label, you can add only devices with an empty label.
NVIDIA GRID vGPU	From the **NVIDIA GRID vGPU Profile** drop-down menu, select the NVIDIA GRID vGPU passthrough device to connect to the virtual machine. **Note:** You can add only one NVIDIA GRID vGPU device in MIG mode to a virtual machine.

5. Click **OK**.
6. Power on the virtual machine.

   The connected PCI devices type appears:

   - On the **Hardware** tab of **Edit Settings** wizard.
   - On the **Summary** tab in the **VM Hardware** panel.

Configuring 3D Graphics

When you create or edit a virtual machine, you can configure 3D graphics to take advantage of Windows AERO, CAD, Google Earth, and other 3D design, modeling, and multimedia applications. Before you enable 3D graphics, become familiar with the available options and requirements.

You can enable 3D on virtual machines that have Windows desktop or Linux guest operating systems. Not all guests support 3D graphics. To verify 3D support for a guest operating system, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Prerequisites

VMware supports AMD and NVIDIA graphics cards. See the vendor website for supported cards. To use the graphics card or GPU hardware, download the appropriate VMware graphics driver from the vendor website.

- Go to the NVIDIA website for information about the VMware graphics driver for your NVIDIA graphics card.
- Go to the AMD website for information about the VMware graphics driver for your AMD graphics card.

Linux distributions must have a 3.2 or later kernel. If 3D is not available on a Linux guest, verify that the driver is available in the Linux kernel. If it is not available, upgrade to a more recent Linux distribution. The location of the kernel depends on whether the distribution is based on `deb` or `rpm` .

Table 161: Linux Driver Location

VMware Linux Guest Kernel Drivers	Debian Format	RPM Format
`vmwgfx.ko`	`dpkg -S vmwgfx.ko`	`rpm -qf vmwgfx.ko`
`vmwgfx_dri.so`	`dpkg -S vmwgfx_dri`	`rpm -qf vmwgfx_dri`
`vmware_drv.so`	`dpkg -S vmware_drv`	`rpm -qf vmware_drv`
`libxatracker.so.1`	`dpkg -S libxatracker`	`rpm -qf libxatracker`

3D Rendering Options

You can select the 3D rendering options for each virtual machine to be Hardware, Software, or Automatic.

Table 162: 3D Rendering Options

Rendering Option	Description
Hardware	The virtual machine must have access to a physical GPU. If the GPU is not available, the virtual machine cannot power on.
Software	The virtual machine's virtual device uses a software renderer and will not attempt to use a GPU, even if one is present.
Automatic	The default setting. The virtual device selects whether to use a physical GPU or software-based rendering. If a GPU is available on the system and has the resources required by the virtual machine, the virtual machine uses the GPU. Otherwise software rendering is used.

How Enabling 3D Graphics Affects the Virtual Machine

You can use vMotion to migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use either the GPU on the destination host or a software renderer, depending on GPU availability. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU.

You can set a group of virtual machines to use only Hardware rendering. For example, if you have virtual machines that run CAD applications or have other complex engineering capabilities, you might require that those virtual machines have persistent high-quality 3D capability present. When you migrate such virtual machines, the destination host must also have GPU capability. If the host does not have GPU, the migration cannot proceed. To migrate such virtual machines, you must turn them off and change the renderer setting to Automatic.

Configure 3D Graphics and Video Cards

When you enable 3D graphics, you can select a hardware or software graphics renderer and optimize the graphics memory allocated to the virtual machine. You can increase the number of displays in multi-monitor configurations and change the video card settings to meet your graphics requirements.

- Verify that the virtual machine is powered off.
- Verify that the virtual machine compatibility is ESXi 5.0 and later.
- To enable 3D graphics in virtual machines with Windows 8 guest operating systems, the virtual machine compatibility must be ESXi 5.1 or later.
- To use a Hardware 3D renderer, ensure that graphics hardware is available. See Configuring 3D Graphics.
- If you update the virtual machine compatibility from ESXi 5.1 and later to ESXi 5.5 and later, reinstall VMware Tools to get the latest SVGA virtual graphics driver and Windows Display Driver Model driver.
- Verify that you have the**Virtual machine** > **Configuration** > **Modify device settings** privilege on the virtual machine.

The default setting for total video RAM is adequate for minimal desktop resolution. For more complex situations, you can change the default memory. Typically, 3D applications require a video memory of 64–512 MB.

Fault Tolerance is not supported for virtual machines that have 3D graphics enabled.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Video Card**.
3. Select custom or automatic settings for your displays from the drop-down menu.

Option	Description
Auto-detect settings	Applies common video settings to the guest operating system.

Option	Description
Specify custom settings	Lets you select the number of displays and the total video memory.

4. Select the number of displays from the drop-down menu.
   You can set the number of displays and extend the screen across them.
5. Enter the required video memory.
6. Optional: Select **Enable 3D support**.
   This check box is active only for guest operating systems on which VMware supports 3D.
7. Optional: Select a 3D Renderer.

Option	Description
Automatic	Selects the appropriate option (software or hardware) for this virtual machine.
Software	Uses normal CPU processing for 3D calculations.
Hardware	Requires graphics hardware (GPU) for faster 3D calculations. **Note:** The virtual machine will not power on if graphics hardware is not available.

8. Click **OK**.

Sufficient memory allocation is set for this virtual machine's graphics.

Reduce Memory Overhead for Virtual Machines with 3D Graphics Option

Virtual machines with the 3D graphics option enabled can have higher memory consumption than other virtual machines. You can reduce the memory overhead by editing the configuration file (`.vmx` file) of your virtual machines and disabling certain memory-related settings. Reducing the memory overhead of virtual machines can help you increase the number of virtual machines per host.

Verify that your virtual machines are using hardware version 10 or later.

1. Shut down the virtual machine on which the 3D graphics option is enabled.
2. Deactivate the **Accelerate 3D Graphics** option.
3. Upgrade your ESXi host to use the features available in hardware version 10 or later.
4. Set the maximum size of your display to the size you need.
5. Locate the configuration file (`.vmx`) of your virtual machine.
6. Open the virtual machine configuration file in a text editor and add the line, `svga.vgaOnly=TRUE`.
   This option removes all graphics and SVGA functionality from your SVGA device, but does not remove the settings that allow BIOS to enter VGA mode.
7. Save the changes and exit the text editor.
8. Power on your virtual machine and check the display console.
9. Verify the memory reservation settings in the `vmware.log` file.

Using a Virtual Watchdog Timer

To ensure self-reliance related to the system performance within a virtual machine, you can add a virtual Watchdog Timer (VWDT) device. If the guest operating system stops responding and cannot recover on its own due to software glitches or errors, the VWDT waits for a predefined period of time and then restarts the system.

You can enable the VWDT to start either by the guest operating system, or by the BIOS or EFI firmware. If you chose the VWDT to start by the BIOS or EFI firmware, it starts before the guest operating system boots.

The VWDT has an important role in guest-based clustering solutions where each virtual machine in the cluster can recover on its own if it fails.

Add a Virtual Watchdog Timer Device to a Virtual Machine

To prevent the virtual machine from a guest operating system failure for an extended period of time, you can add a VWDT device to the virtual machine.

- Power off the virtual machine.
- Verify that the virtual machine hardware is of version 17 or later.
- Verify that the guest operating system of the virtual machine supports a watchdog timer:
  Note: The guest operating system may require you to explicitly enable the watchdog services. Failure to do so might cause the watchdog timer to power off or restart the virtual machine.
  - The VWDT device implements the Watchdog Resource Table (WDRT) and Watchdog Action Table (WDAT) specifications. Windows Server 2003 supports devices compatible with WDRT and Windows Server 2008 and later supports devices compatible with WDAT.
  - The Linux distributions based on 4.9 or later kernel, such as Ubuntu 18.04 and Red Hat Enterprise Linux 7.6, support devices compatible with WDAT if the `wdat_wdt.ko` driver is available.
  - The watchdog timer is not supported for other guest operating systems, such as FreeBSD and Mac OS X.
- Required privileges:
  - **Virtual Machine** > **Configuration** > **Add or remove device**
  - **Virtual machine** > **Configuration** > **Modify device settings**

1. Right-click a virtual machine from the vSphere inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click **Add New Device** and select **Watchdog Timer** from the drop-down menu.
   The New Watchdog timer device appears in the **Virtual Hardware** devices list.
3. To start the virtual watchdog timer with the BIOS or EFI firmware, select **Start with BIOS/EFI boot**.
   The virtual watchdog timer starts before the guest operating system boots.

   If the guest operating system takes too long to boot or it does not support the VWDT device, a warning message appears, and the VWDT device might constantly restart the virtual machine.
4. Click **OK**.

You can view the status of the VWDT device in the **VM Hardware** panel on the **Summary** tab.

Add a Precision Clock Device to a Virtual Machine

A Precision Clock device is a virtual clock device that provides a virtual machine with access to the system time of the primary host.

- To ensure that the Precision Clock device provides the guest operating system of a virtual machine with accurate time, synchronize the primary host to use Network Time Protocol (NTP) or Precision Time Protocol (PTP). For information how to configure the host time synchronization, see the *vSphere Single Host Management - VMware Host Client* documentation.
- Power off the virtual machine.
- Verify that the virtual machine hardware is of version 17.

- Required privileges:
  - **Virtual Machine** > **Configuration** > **Add or remove device**
  - **Virtual machine** > **Configuration** > **Modify device settings**

To synchronize the guest operating system of a virtual machine with the host in an efficient manner, add a Precision Clock device to the virtual machine. For information on how to use the Precision Clock device as a reference clock for time synchronization of the supported guest operating system, see the *vCenter Server and Host Management* documentation.

1. Right-click a virtual machine from the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click **Add New Device**, and from the drop-down menu select **Precision Clock**.
   The Precision Clock device appears in the **Virtual Hardware** devices list.
3. Select the time synchronization protocol and click **OK**.

Option	Description
Any	The host time synchronization type has no limitations.
NTP	You can power on the virtual machine on an host that is configured with NTP time synchronization.
PTP	You can power on the virtual machine on an host that is configured with PTP time synchronization.

Securing Virtual Machines with Intel Software Guard Extensions

By using the , you can configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines and provide additional security to your workloads.

Some modern Intel CPUs implement a security extension called Intel® Software Guard Extensions (Intel SGX). Intel SGX is a processor-specific technology that defines private regions of memory, called enclaves. Intel SGX protects the enclave contents from disclosure and modification in such a way that code running outside the enclave cannot access them.

vSGX enables virtual machines to use Intel SGX technology if available on the hardware. To use vSGX, the ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the BIOS of the ESXi host. You can use the vSphere Client to enable SGX for a virtual machine.

Enable vSGX on a Virtual Machine

You can enable vSGX on a virtual machine when you deploy a virtual machine, edit or clone an existing virtual machine.

To use vSGX, your environment must meet a list of requirements.

- The ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the BIOS of the ESXi host. For information about the supported CPUs, see the VMware KB article at https://kb.vmware.com/s/article/71367.
- Verify that the ESXi host is ESXi 7.0 or later.
- The guest operating system of the virtual machine must be Linux, Windows 10 (64-bit) and later, or Windows Server 2016 (64-bit) and later.
- Verify that the virtual machine hardware is of version 17.
- Verify that the virtual machine uses EFI firmware.
- Verify that the virtual machine is powered off.
- Verify that you have the privileges to create, clone, or edit virtual machine settings. For more information, see Create a Virtual Machine with the New Virtual Machine Wizard and Clone an Existing Virtual Machine.

Note: Some operations and features are not supported for a virtual machine when vSGX is enabled.

- Migration with Storage vMotion.
- Suspending or resuming the virtual machine.
- Taking snapshot of the virtual machine, especially if you take a snapshot of the virtual machine memory.

- Fault Tolerance
- Enabling Guest Integrity (GI, platform foundation for VMware AppDefense™ 1.0).

1. You can enable SGX when you deploy a virtual machine or edit an existing virtual machine.

Option	Action
Deploy a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine and select **New Virtual Machine**. 2. On the **Select a creation type** page, select **Create a new virtual machine**, and click **Next**. 3. Navigate through the pages of the wizard. 4. On the **Customize hardware** page, click the **Virtual Hardware** tab.
Edit a virtual machine	1. Right-click a virtual machine in the inventory and select **Edit Settings**. 2. Click the **Virtual Hardware** tab.
Clone an existing virtual machine	1. Right-click a virtual machine in the inventory and select **Clone** > **Clone to Virtual Machine**. 2. Navigate through pages of the wizard. 3. On the **Select clone options** page, select **Customize this virtual machine's hardware** and click **Next**. 4. Click the **Virtual Hardware** tab.

2. On the **Virtual Hardware** tab, expand **Security Devices**.
3. To enable SGX, select the **Enable** check box.
4. In the **Enclave page cache size (MB)** text box, enter the size of the cache size in MB.

   Note: The enclave page cache size must be multiple of 2 MB.
5. From the **Launch control configuration** drop-down menu, select the appropriate mode.

Option	Action
Unlocked	This option enables the launch enclave configuration of the guest operating system.
Locked	This option allows you to configure the launch enclave. 1. Select the **Launch enclave public key hash** option. 2. To use one of the public keys configured on the host, select **Use from host** and from the drop-down menu, select a public key hash. 3. To enter the public key manually, select **Enter manually** and enter a valid SHA256 hash (64) characters key.

6. Click **OK**.

Remove vSGX from a Virtual Machine

You can remove vSGX from a virtual machine.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Security Devices**.
3. Deselect the **Enable** check box for SGX and click **OK**.

You removed vSGX from the virtual machine. The vSGX no longer appears on the virtual machine **Summary** tab of the **VM Hardware** pane.

USB Configuration from an ESXi Host to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices are connected to an ESXi host. USB passthrough technology supports adding USB devices, such as security dongles and mass storage devices, to virtual machines that reside on the host to which the devices are connected.

How USB Device Passthrough Technology Works

When you attach a USB device to a physical host, the device is available only to virtual machines that reside on that host. The device cannot connect to virtual machines that reside on another host in the data center.

A USB device is available to only one virtual machine at a time. When you connect a device to a powered on virtual machine, the device is not available to connect to other virtual machines that run on the host. When you remove the active connection of a USB device from a virtual machine, it becomes available to the other virtual machines that run on the host.

To connect a USB passthrough device to a virtual machine that runs on the ESXi host where the device is physically attached, you require an arbitrator, a controller, and a physical USB device or device hub.

USB Arbitrator	Manages connection requests and routes the USB device traffic. The arbitrator is installed and enabled by default on ESXi hosts. It scans the host for USB devices and manages the device connection among virtual machines that reside on the host. It routes the device traffic to the correct virtual machine for delivery to the guest operating system. The arbitrator monitors the USB device and prevents other virtual machines from using it until you release it from the virtual machine it is connected to.
USB Controller	The USB hardware chip that provides a USB function to the USB ports that it manages. The virtual USB controller is the software virtualization of the USB host controller function in the virtual machine. USB controller hardware and modules that support USB devices, such as USB 3.1 SuperSpeedPlus, USB 3.1 SuperSpeed, USB 2.0, and USB 1.1 must exist on the host. A controller must be present before you can add a USB device to the virtual machine. The USB arbitrator can monitor a maximum of 15 USB controllers. Devices connected to controllers numbered 16 or greater are not available to the virtual machine.
USB Devices	You can add up to 20 USB devices to a virtual machine, which is the maximum number of devices supported for a simultaneous connection to one virtual machine. The maximum number of USB devices supported on a single ESXi host for a simultaneous connection to one or more virtual machines is also 20. For more information, see Supported USB device models for passthrough from an ESX or ESXi host to a virtual machine.

USB 3.1 SuperSpeed Device Requirements

Starting with vSphere 5.5 Patch 3, USB 3.1 SuperSpeed devices are available for passthrough not only from a client computer to a virtual machine, but also from an ESXi host to a virtual machine. USB 3.1 SuperSpeed devices still have the following virtual machine configuration requirement:

- The virtual machine must have an enabled xHCI controller, Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.

USB 3.1 SuperSpeedPlus Device Requirements

Starting with vSphere 7.0, USB 3.1 SuperSpeedPlus devices are available for passthrough at their maximum speed (SuperSpeedPlus), not only from a client computer to a virtual machine, but also from an ESXi host to a virtual machine. To operate their maximum transfer speed, USB 3.1 SuperSpeedPlus devices have the following virtual machine configuration requirements:

- The virtual machine must have an enabled xHCI controller, Windows 10 or later, Windows Server 2016 and later, or a Linux guest operating system with a 4.6 or later kernel.
- Verify that the virtual machine hardware is of version 17 or later.
- For requirements and steps how to enable USB 3.1 SuperSpeedPlus, see the VMware knowledge base article https://kb.vmware.com/s/article/70748.

USB Autoconnect Feature

When you add a USB device connection from an ESXi host to a virtual machine, the autoconnect feature is activated for the device connection. It is not deactivated until you remove the device connection from the virtual machine.

With autoconnect enabled, the device reconnects in the following cases:

- The virtual machine is cycling through power operations, such as Power Off/Power On, Reset, Pause/Resume.
- The device is unplugged from the host, and then plugged back in to the same USB port.
- The device is power cycled but has not changed its physical connection path.
- The device is mutating identity while it is in use.
- A new virtual USB device is added.

The USB passthrough autoconnect feature identifies the device by using the USB path of the device on the host. It uses the physical topology and port location instead of the device identity.

If you plug the same device back in to a different USB port on the host, it cannot reestablish the connection with the virtual machine. If you unplug the device from the host and plug in a different device to the same USB path, the new device appears. It is connected to the virtual machine by the autoconnect feature that you enabled in the previous device connection.

Autoconnect is useful when devices mutate during usage. For example, for iPhones and other similar devices, the device VID/PID changes during software or firmware upgrades. The upgrade process disconnects and reconnects the devices to the USB port.

The USB port is speed-specific. If you change a USB device with another USB device that works with different speed, the autoconnect feature might not work. For example, you might connect a USB 2.0 high-speed device to a port and connect that device to the virtual machine. If you unplug the device from the host and plug in a USB 1.1, USB 3.1 SuperSpeed, or 3.1 SuperSpeedPlus device to the same port, the device might not connect to the virtual machine.

For a list of supported USB devices for passthrough from an ESXi host to a virtual machine, see Supported USB device models for passthrough from an ESX or ESXi host to a virtual machine.

vSphere Features Available with USB Passthrough

Migrations with vMotion and DRS are supported with USB device passthrough from an ESXi host to a virtual machine.

Table 163: vSphere Features Available for USB Passthrough from an ESXi Host to a Virtual Machine

Feature	Supported with USB Device Passthrough
vSphere Distributed Power Management (DPM)	No
vSphere Distributed Resource Scheduler (DRS)	Yes
vSphere Fault Tolerance	No
vSphere vMotion	Yes

For details about migration with vMotion, see Conditions and Limitations When Configuring USB Devices for vMotion.

If a host with connected USB devices resides in a DRS cluster with activated DPM, you must deactivate DPM for that host. Otherwise DPM might power off the host with the device, which disconnects the device from the virtual machine.

Conditions and Limitations When Configuring USB Devices for vMotion

With USB passthrough from a host to a virtual machine, you can migrate a virtual machine to another ESXi host in the same datacenter and maintain the USB passthrough device connections to the original host.

If a virtual machine has USB devices attached that pass through to an ESXi host, you can migrate that virtual machine with the devices attached.

For a successful migration, review the following conditions:

- You must configure all USB passthrough devices connected to a virtual machine for vMotion. If one or more devices is not configured for vMotion, the migration cannot proceed. For troubleshooting details, see the Troubleshooting USB Passthrough Devices documentation.
- When you migrate a virtual machine with attached USB devices away from the host to which the devices are connected, the devices remain connected to the virtual machine. However, if you suspend or power off the virtual machine, the USB devices are disconnected and cannot reconnect when the virtual machine is resumed. The device connections can be restored only if you move the virtual machine back to the host to which the devices are attached.
- If you resume a suspended virtual machine that has a Linux guest operating system, the resume process might mount the USB devices at a different location on the file system.
- If a host with attached USB devices resides in a DRS cluster with activated distributed power management (DPM), deactivate DPM for that host. Otherwise DPM might turn off the host with the attached device. This action disconnects the device from the virtual machine because the virtual machine migrated to another host.
- Remote USB devices require that the hosts be able to communicate over the management network following migration with vMotion, so the source and destination management network IP address families must match. You cannot migrate a virtual machine from a host that is registered to vCenter Server with an IPv4 address to a host that is registered with an IPv6 address.

Avoiding Data Loss with USB Devices

When a virtual machine connects to a physical UBS device on an ESXi host, virtual machine functions can affect USB device behavior and connections.

- Before you hot add memory, CPU, or PCI devices, you must remove any USB devices. Hot adding these resources disconnects USB devices, which might result in data loss.
- Before you suspend a virtual machine, make sure that a data transfer is not in progress. During the suspend or resume process, USB devices behave as if they have been disconnected, then reconnected. For information about suspend

and resume behavior after migration with vMotion, see Conditions and Limitations When Configuring USB Devices for vMotion.

- Before you change the state of the arbitrator, make sure that USB devices residing on the host are not attached to a virtual machine. If USB devices become unavailable to a virtual machine, a host administrator might have deactivated the arbitrator. When an administrator stops or disconnects the arbitrator for troubleshooting or other purposes, USB devices attached to that host become unavailable to the virtual machine. If a data transfer is taking place at this time, you might lose the data. To reestablish the arbitrator, you must restart the host or restart the `usbarbitrator` and `hostd` services. Restarting the services requires that you power off and then power on the virtual machine.

Connecting USB Devices to an ESXi Host

You can connect and chain multiple USB hubs and devices to an ESXi host. Careful planning and knowledge of hub behavior and limitations can help ensure that your devices work optimally.

USB physical bus topology defines how USB devices connect to the host. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the host does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the host USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Communication delay between the host and virtual machine increases as the number of cascading hubs increases.
- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.
- Chaining hubs together also increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.
- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the host rather than to a hub or extension cable might resolve their connection or performance issues.

Note: To prevent additional problems, be aware of the physical constraints of long-term deployment in a machine room environment. Small devices are easily damaged by being stepped on or knocked loose.

In some cases, you must hard reset the device and hub to restore the device to a working state.

For a list of supported USB devices for passthrough from an ESXi host to a virtual machine, see the VMware knowledge base article at http://kb.vmware.com/kb/1021345.

USB Compound Devices

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

Add USB Devices to an ESXi Host

You can connect multiple USB devices to an ESXi host so that the virtual machines that run on the same host can access the devices. The number of devices that you can connect depends on the device type and how the devices and hubs chain together.

- If a host has attached USB devices and resides in a DRS cluster with activated DPM, deactivate DPM for that host. For instructions about overriding the default DPM setting for a single host, see *vSphere Resource Management*.
- To verify that the virtual machine meets the requirements for the USB device connection, see Connecting USB Devices to an ESXi Host.
- To add eight xHCI controllers to the ESXi host, verify that the current version of your ESXi host is 6.0 or later.

Each ESXi host has several USB ports. The number of ports on each host depends on the physical setup of the host. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes more than 15 controllers and you connect USB devices to them, the devices are not available to the virtual machine.

The host treats USB CD/DVD-ROM devices as SCSI devices.

- To add a USB device to an ESXi host, connect the device to an available port or hub.

You can add the device to the virtual machine. See Add USB Devices from an ESXi Host to a Virtual Machine.

Add a USB Controller to a Virtual Machine

To support USB passthrough from an ESXi host or from a client computer to a virtual machine, you can add a USB controller to the virtual machine.

- Verify that the ESXi hosts have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices.
- Verify that the client computers have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, verify that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine** > **Configuration** > **Add or Remove Device**

In the vSphere Client, you can add one xHCI controller and one EHCI+UHCI controller. From hardware version 11 to hardware version 16, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeed ports and four logical USB 2.0 ports). With hardware version 17, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeedPlus ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 164: USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to a VM	Supported for Passthrough from Client Computer to a VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.1, 2.0, and 1.1	Yes USB 3.1, 2.0, and 1.1 devices only.	Yes Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for access to a USB mouse and keyboard.

For virtual machines with Windows or Linux guest operating systems, you can add one or two controllers of different types. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes more than 15 controllers and you connect USB devices to them, the devices are not available to the virtual machine.

1. Right-click a virtual machine from the vSphere inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click **Add New Device** and from the drop-down menu select **USB Controller**.
   The controller appears in the **Virtual Hardware** devices list.
3. To change the USB controller type, expand **New USB Controller**.
4. Click **OK**.

Add one or more USB devices to the virtual machine.

Add USB Devices from an ESXi Host to a Virtual Machine

You can add one or more USB passthrough devices from an ESXi host to a virtual machine if the physical devices are connected to the host on which the virtual machine runs.

- Verify that the virtual machine is compatible with ESX/ ESXi 4.0 and later.
- Verify that a USB controller is present. See Add a USB Controller to a Virtual Machine.
- To use vMotion to migrate a virtual machine with multiple USB devices, enable all attached USB devices for vMotion. You cannot migrate individual USB devices. For vMotion limitations, see Conditions and Limitations When Configuring USB Devices for vMotion.
- When you add a CD/DVD-ROM drive that is backed by a USB CD/DVD drive on the host, add the drive as a SCSI device. Hot adding and removing SCSI devices is not supported.
- Verify that you know the virtual machine requirements for USB devices. See USB Configuration from an ESXi Host to a Virtual Machine.
- Required privileges: **Virtual Machine** > **Configuration** > **HostUSBDevice**

If a USB device is connected to another virtual machine, you cannot add it until that machine releases it.

Note:

If you have the Apple Frontpanel Controller device in your environment, you can safely add it to a virtual machine. However, this device has no documented function and no known use. ESXi hosts do not use it and do not provide Xserver functionality for USB passthrough.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click the **Add New Device** button.
3. Select **Host USB Device** from the drop-down menu.
   The new USB device appears at the bottom of the Virtual Hardware device list.
4. Expand **New USB Device**, and select the device to add.
   You can add multiple USB devices, but only one device at a time.
5. If you do not plan to migrate a virtual machine with USB devices attached, deselect the **Support vMotion** option.
   This action reduces migration complexity, which results in better performance and stability.

6. Click **OK**.

Remove USB Devices That Are Connected Through an ESXi Host

When you remove USB devices from a virtual machine, devices that use passthrough technology from a host to the virtual machine revert to the host. The devices become available to other virtual machines that run on that host.

- Verify that the devices are not in use.
- To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a Remove Hardware icon located in the System Tray. Linux operating systems use the `umount` command.
  Note: You might need to use the `sync` command instead of or in addition to the `umount` command, for example, after you issue a `dd` command on Linux or other UNIX operating systems.

1. Unmount or eject the USB device from the guest operating system.
2. Right-click a virtual machine in the inventory and select **Edit Settings**.
3. To remove the device, move the pointer over the device and click the **Remove** icon.
4. Click **OK** to save your changes.

Remove USB Devices from an ESXi Host

You can remove USB devices from the host if you must shut down the host for maintenance or if you do not want those devices to be available to virtual machines that run on the host. When you detach a USB device from the host, the device disconnects from the virtual machine.

Verify that the USB devices are not in use.

CAUTION: If data transfer is taking place when you remove USB devices from a host, you can lose data.

- Follow the device manufacturers instructions to safely remove the device.
  When you remove the device from the host, it is no longer available to the virtual machines that run on the host.

USB Configuration from a Client Computer to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices are connected to the client computer on which you run the vSphere Client. The vSphere Client must be logged in to a vCenter Server instance that manages the ESXi host where the virtual machine resides. USB passthrough technology supports adding multiple USB devices, such as security dongles, mass storage devices, and smartcard readers to virtual machines.

How USB Device Passthrough Technology Works

The USB controller is the USB hardware chip that provides a USB function to the USB ports that it manages. The USB controller hardware and modules that support USB 3.1 SuperSpeedPlus, USB 3.1 SuperSpeed, 2.0, and USB 1.1 devices must be available on the virtual machine. Two USB controllers are available for each virtual machine. The controllers support multiple USB devices, such as USB 3.1 SuperSpeedPlus, USB 3.1 SuperSpeed, 2.0, and 1.1. The controller must be present before you can add USB devices to the virtual machine.

You can add up to 20 USB devices to a virtual machine, which is the maximum number of devices supported for a simultaneous connection to one virtual machine. You can add the devices only one at a time.

The virtual machine retains its connection to the device while it is in an S1 standby state. USB device connections are preserved when you migrate virtual machines to another host in the data center.

A USB device is available to only one powered on virtual machine at a time. When a virtual machine connects to a device, that device is no longer available to other virtual machines or to the client computer. When you disconnect the device from

the virtual machine or shut down the virtual machine, the device returns to the client computer and becomes available to other virtual machines that the client computer manages.

For example, when you connect a USB mass storage device to a virtual machine, it is removed from the client computer and does not appear as a drive with a removable device. When you disconnect the device from the virtual machine, it reconnects to the client computer's operating system and is listed as a removable device.

USB 3.1 SuperSpeed Device Requirements

Starting with vSphere 5.5 Patch 3, USB 3.1 SuperSpeed devices are available for passthrough not only from a client computer to a virtual machine, but also from an ESXi host to a virtual machine. USB 3.1 SuperSpeed devices still have the following virtual machine configuration requirement:

- The virtual machine must have an enabled xHCI controller, Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.

Avoiding Data Loss

Before you connect a device to a virtual machine, make sure that the device is not in use on the client computer.

If the vSphere Client disconnects from the vCenter Server system or host, or if you restart or shut down the client computer, the device connection breaks. It is best to have a dedicated client computer for USB device use or to reserve USB devices connected to a client computer for short-term use, such as updating software or adding patches to virtual machines. To maintain USB device connections to a virtual machine for an extended time, use USB passthrough from an ESXi host to the virtual machine.

USB 3.1 SuperSpeedPlus Device Requirements

Starting with vSphere 7.0, USB 3.1 SuperSpeedPlus devices are available for passthrough at their maximum speed (SuperSpeedPlus), not only from a client computer to a virtual machine, but also from an ESXi host to a virtual machine. To operate their maximum transfer speed, USB 3.1 SuperSpeedPlus devices have the following virtual machine configuration requirements:

- The virtual machine must have an enabled xHCI controller, Windows 10 or later, Windows Server 2016 and later, or a Linux guest operating system with a 4.6 or later kernel.
- Verify that the virtual machine hardware is of version 17 or later.
- For requirements and steps how to enable the USB 3.1 SuperSpeedPlus, see the VMware knowledge base article https://kb.vmware.com/s/article/70748.

Connecting USB Devices to a Client Computer

You can connect and chain any multiple low, full, and high- or super-speed USB hubs and devices to a client computer. Careful planning and knowledge of hub behavior and limitations can help ensure that your devices work optimally.

USB physical bus topology defines how USB devices connect to the client computer. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the client computer does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the client computer USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.

- Chaining hubs together increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.
- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the client computer rather than to a hub or extension cable might resolve their connection or performance issues. In some cases, you must remove and reattach the device and hub to restore the device to a working state.

USB Compound Devices

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

Connect a USB Device to a Client Computer

You can connect multiple USB devices to a client computer so that virtual machines can access the devices. The number of devices that you can add depends on several factors, such as how the devices and hubs chain together and the device type.

USB physical bus topology defines how USB devices connect to the client computer. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the client computer does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the client computer USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.
- Chaining hubs together increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.
- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the client computer rather than to a hub or extension cable might resolve their connection or performance issues. In some cases, you must remove and reattach the device and hub to restore the device to a working state.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15-controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

To add a USB device to a client computer, connect the device to an available port or hub.

You can now add the USB device to the virtual machine.

Add a USB Controller to a Virtual Machine

To support USB passthrough from an ESXi host or from a client computer to a virtual machine, you can add a USB controller to the virtual machine.

- Verify that the ESXi hosts have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices.
- Verify that the client computers have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, verify that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine** > **Configuration** > **Add or Remove Device**

In the vSphere Client, you can add one xHCI controller and one EHCI+UHCI controller. From hardware version 11 to hardware version 16, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeed ports and four logical USB 2.0 ports). With hardware version 17, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeedPlus ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 165: USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to a VM	Supported for Passthrough from Client Computer to a VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.1, 2.0, and 1.1	Yes USB 3.1, 2.0, and 1.1 devices only.	Yes Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for access to a USB mouse and keyboard.

For virtual machines with Windows or Linux guest operating systems, you can add one or two controllers of different types. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes more than 15 controllers and you connect USB devices to them, the devices are not available to the virtual machine.

1. Right-click a virtual machine from the vSphere inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click **Add New Device** and from the drop-down menu select **USB Controller**.
   The controller appears in the **Virtual Hardware** devices list.
3. To change the USB controller type, expand **New USB Controller**.
4. Click **OK**.

Add one or more USB devices to the virtual machine.

Add USB Devices from a Client Computer to a Virtual Machine

You can add one or more USB passthrough devices from a client computer to a virtual machine in the vSphere Client. The devices must be connected to a client computer that connects to the ESXi host on which the virtual machine resides.

- Verify that a USB device is connected to the client computer.
- Verify that the virtual machine is powered on.
- Verify that a USB controller is present.

Note: If you connect to a USB device on a Mac OS X client computer, you can add only one device to the virtual machine at a time.

The devices maintain their virtual machine connections in S1 standby, if the vSphere Client is running and connected. After you add the USB device to the virtual machine, a message on the client computer states that the device is disconnected. The device remains disconnected from the client computer until you disconnect it from the virtual machine.

Fault Tolerance is not supported with USB passthrough from a client computer to a virtual machine.

1. In the vSphere Client, navigate to a virtual machine.
2. Launch the VMware Remote Console application.

   Note: You cannot connect a USB device to a virtual machine if you use the HTML5 console in the vSphere Client.
3. In the VMware Remote Console toolbar, click **VMRC** > **Removable Devices** and find the USB device.
4. Click **Connect (Disconnect from menu)**.

The USB device is connected to the virtual machine.

Remove USB Devices That Are Connected Through a Client Computer

You can remove USB devices from a virtual machine if the devices are no longer needed. When you disconnect a USB device from a virtual machine, the device is released from the virtual machine and is given back to the client computer, which starts using it.

1. Unmount or eject the USB device from the guest operating system.
2. On the virtual machine **Summary** tab, click the disconnect icon on the right side of the USB device entry.
3. Select a device to disconnect from the drop-down menu.

   A **Disconnecting** label and a spinner appear, indicating that a disconnection is in progress. When the device is disconnected, after a slight delay, the **Summary** tab refreshes and the device is removed from the virtual machine configuration.

The device reconnects to the client computer and is available to add to another virtual machine. In some cases, Windows Explorer detects the device and opens a dialog box on the client computer. You can close this dialog box.

Remove a USB Controller from a Virtual Machine

You can remove a USB controller from the virtual machine if you do not want to connect to USB devices.

Note: The ESXi host supports hot-removal of a USB controller. You can remove a USB controller from a virtual machine when both the ESXi host and the guest operating system of the virtual machine support the hot-removal functionality.

To make sure that the guest operating system of the virtual machine supports the hot-removal functionality, refer to the vendors documentation.

- Verify that the USB controller is not in use.

- Verify that all USB devices are disconnected from the virtual machine.
- Required Privilege: **Virtual Machine** > **Configuration** > **Add or Remove Device**

1. Navigate to a data center, folder, cluster, resource pool, host, or vApp, click the **VMs** tab and click **Virtual Machines**.
2. Right-click a virtual machine and click **Edit Settings**.
3. On the **Virtual Hardware** tab, move the pointer over the USB controller and click the **Remove** icon.
4. Click **OK** to confirm the deletion and close the dialog box.

The controller is no longer connected to the virtual machine, but remains available to add at a later time.

Add a Shared Smart Card Reader to Virtual Machines

You can configure multiple virtual machines to use a virtual shared smart card reader for smart card authentication. The smart card reader must be connected to a client computer on which the vSphere Client runs. All smart card readers are treated as USB devices.

- Verify that the smart card reader is connected to the client computer.
- Verify that the virtual machine is powered on.
- Verify that a USB controller is present.
- Required Privilege: **Virtual machine** > **Configuration** > **Add or remove device**

A license is required for the shared smart card feature. See *vCenter Server and Host Management*.

When you log out of Windows XP guest operating systems, to log back in, you must remove the smart card from the smart card reader and re-add it. You can also disconnect the shared smart card reader and reconnect it.

If the vSphere Client disconnects from the vCenter Server or host, or if the client computer is restarted or shut down, the smart card connection breaks. For this reason, it is best to have a dedicated client computer for smart card use.

To connect a USB smart card reader that is not shared, see USB Configuration from a Client Computer to a Virtual Machine.

1. Navigate to a datacenter, folder, cluster, resource pool, host, or vApp, and click the **Related Options** tab and click **Virtual Machines**.
2. Select a virtual machine, click it again, and click the **Summary** tab.
3. Click the USB icon on the right side of **USB Devices** under **VM Hardware**, and select an available shared smart card reader from the drop down menu.

   Select a device that appears as **Shared** ***`the model name of your smart card reader`*** followed by a number.

   A **Connecting** label and a spinner appear showing that a connection is in progress. When the device has successfully connected and the Summary tab refreshes, the device is connected and the device name appears next to **USB Devices**.

You can now use smart card authentication to log in to virtual machines in the vSphere Client inventory.

Securing Virtual Machines with Virtual Trusted Platform Module

With the Virtual Trusted Platform Module (vTPM) feature, you can add a TPM 2.0 virtual cryptoprocessor to a virtual machine.

A vTPM is a software-based representation of a physical Trusted Platform Module 2.0 chip. A vTPM acts as any other virtual device. You can add a vTPM to a virtual machine in the same way you add virtual CPUs, memory, disk controllers, or network controllers. A vTPM does not require a hardware Trusted Platform Module chip.

Virtual Trusted Platform Module Overview

A virtual Trusted Platform Module (vTPM) is a software-based representation of a physical Trusted Platform Module 2.0 chip. A vTPM acts as any other virtual device.

What Is a vTPM

vTPMs provide hardware-based, security-related functions such as random number generation, attestation, key generation, and more. When added to a virtual machine, a vTPM enables the guest operating system to create and store keys that are private. These keys are not exposed to the guest operating system itself. Therefore, the virtual machine attack surface is reduced. Usually, compromising the guest operating system compromises its secrets, but enabling a vTPM greatly reduces this risk. These keys can be used only by the guest operating system for encryption or signing. With an attached vTPM, a client can remotely attest the identity of the virtual machine, and verify the software that it is running.

You can add a vTPM to either a new or an existing virtual machine. A vTPM depends on virtual machine encryption to secure vital TPM data. When you configure a vTPM, the virtual machine files are encrypted but not the disks. You can choose to add encryption explicitly for the virtual machine and its disks.

When you back up a virtual machine enabled with a vTPM, the backup must include all virtual machine data, including the `*.nvram` file. If your backup does not include the `*.nvram` file, you cannot restore a virtual machine with a vTPM. Also, because the VM home files of a vTPM-enabled virtual machine are encrypted, ensure that the encryption keys are available at the time of a restore.

Note: By default, no storage policy is associated with a virtual machine that has been enabled with a vTPM. Only the virtual machine files (VM Home) are encrypted. If you prefer, you can choose to add encryption explicitly for the virtual machine and its disks, but the virtual machine files would have already been encrypted.

vSphere Requirements for vTPMs

To use a vTPM, your vSphere environment must meet these requirements:

- Virtual machine requirements:
  - EFI firmware
  - Hardware version 14 and later
- Component requirements:
  - vCenter Server 6.7 and later for Windows virtual machines, vCenter Server 7.0 Update 2 and later for Linux virtual machines.
  - Virtual machine encryption (to encrypt the virtual machine home files).
- Guest OS support:
  - Linux
  - Windows Server 2008 and later
  - Windows 7 and later

Differences between a Hardware TPM and a Virtual TPM

You use a hardware Trusted Platform Module (TPM) to provide secure storage of credentials or keys. A vTPM performs the same functions as a TPM, but it performs cryptographic coprocessor capabilities in software. A vTPM uses the `.nvram` file, which is encrypted using virtual machine encryption, as its secure storage.

A hardware TPM includes a preloaded key called the Endorsement Key (EK). The EK has a private and public key. The EK provides the TPM with a unique identity. For a vTPM, this key is provided either by the VMware Certificate Authority (VMCA) or by a third-party Certificate Authority (CA). After the vTPM uses a key, it is typically not changed because doing so invalidates sensitive information stored in the vTPM. The vTPM does not contact the third-party CA at any time.

Create a Virtual Machine with a Virtual Trusted Platform Module

You can add a Virtual Trusted Platform Module (vTPM) when you create a virtual machine to provide enhanced security to the guest operating system. You must create a key provider before you can add a vTPM.

- The guest OS you use can be Windows Server 2008 and later, Windows 7 and later, or Linux.
- The ESXi hosts running in your environment must be ESXi 6.7 or later (Windows guest OS), or 7.0 Update 2 (Linux guest OS).
- The virtual machine must use EFI firmware.
- Verify that you have the required privileges:
  - **Cryptographic operations** > **Clone**
  - **Cryptographic operations** > **Encrypt**
  - **Cryptographic operations** > **Encrypt new**
  - **Cryptographic operations** > **Migrate**
  - **Cryptographic operations** > **Register VM**

Note: After creating a virtual machine with a vTPM, the**Cryptographic operations** > **Direct Access** privilege is required to open a console session.

The VMware virtual TPM is compatible with TPM 2.0 and creates a TPM-enabled virtual chip for use by the virtual machine and the guest OS it hosts.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object, select **New Virtual Machine**, and follow the prompts to create a virtual machine.

Option	Action
Select a creation type	Create a new virtual machine.
Select a name and folder	Specify a name and target location.
Select a compute resource	
Select storage	Select a compatible datastore.
Select compatibility	You must select **ESXi 6.7 and later** for Windows guest OS, or **ESXi 7.0 U2** and later for Linux guest OS.
Select a guest OS	Select Windows or Linux for use as the guest OS.
Customize hardware	Click **Add New Device** and select **Trusted Platform Module**. You can further customize the hardware, for example, by changing disk size or CPU.
Ready to complete	Review the information and click **Finish**.

The vTPM-enabled virtual machine appears in your inventory as specified.

Enable Virtual Trusted Platform Module for an Existing Virtual Machine

You can add a Virtual Trusted Platform Module (vTPM) to an existing virtual machine to provide enhanced security to the guest operating system. You must create a key provider before you can add a vTPM.

- The guest OS you use can be Windows Server 2008 and later, Windows 7 and later, or Linux.
- Verify that the virtual machine is turned off.
- The ESXi hosts running in your environment must be ESXi 6.7 or later (Windows guest OS), or 7.0 Update 2 (Linux guest OS).
- The virtual machine must use EFI firmware.

- Verify that you have the required privileges:
  - **Cryptographic operations** > **Clone**
  - **Cryptographic operations** > **Encrypt**
  - **Cryptographic operations** > **Encrypt new**
  - **Cryptographic operations** > **Migrate**
  - **Cryptographic operations** > **Register VM**
  - **Virtual machine** > **Configuration** > **Add or remove device**

Note: After adding a vTPM to a virtual machine, the **Cryptographic operations** > **Direct Access** privilege is required to open a console session.

The VMware virtual TPM is compatible with TPM 2.0, and creates a TPM-enabled virtual chip for use by the virtual machine and the guest OS it hosts.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, click **Add New Device** and select **Trusted Platform Module**.
4. Click **OK**.

   The virtual machine **Summary** tab now includes Virtual Trusted Platform Module in the **VM Hardware** pane.

Remove Virtual Trusted Platform Module from a Virtual Machine

You can remove Virtual Trusted Platform Module (vTPM) security from a virtual machine.

- Ensure that the virtual machine is powered off.
- Verify that you have the required privilege: **Cryptographic operations** > **Decrypt**

Removing a vTPM device causes all encrypted information on the virtual machine to become unrecoverable. Before removing a vTPM from a virtual machine, deactivate any applications in the Guest OS that use the vTPM device, such as BitLocker. Failure to do so can cause the virtual machine not to boot. Also, you cannot remove a vTPM from a virtual machine that contains snapshots.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, locate the Trusted Platform Module entry in the **Virtual Hardware** tab.
4. Move your pointer over the device and click the **Remove** icon.

   This icon appears only for the virtual hardware that you can safely remove.
5. Click **Delete** to confirm you want to remove the device.

   The vTPM device is marked for removal.
6. Click **OK**.

   Verify that the Virtual Trusted Platform Module entry no longer appears in the virtual machine **Summary** tab in the **VM Hardware** pane.

Identify Virtual Trusted Platform Module Enabled Virtual Machines

You can identify which of your virtual machines are enabled to use a Virtual Trusted Platform Module (vTPM).

You can generate a list of all virtual machines in your inventory showing virtual machine name, operating system, and vTPM status. You can also export this list to a CSV file for use in compliance audits.

1. Connect to vCenter Server by using the vSphere Client.
2. Select a vCenter Server instance, a host, or a cluster.
3. Click the **VMs** tab and click **Virtual Machines**.
4. To view all virtual machines on which a TPM is enabled, click the three-bar **Column Selector** in the lower left corner and select **TPM**.

   The TPM column displays "Present" for virtual machines on which a TPM is enabled. Virtual machines without a TPM are listed as "Not present."
5. You can export the contents of an inventory list view to a CSV file.
   a) Click **Export** at the bottom-right corner of a list view.

      The Export List Contents dialog box opens and lists the available options for inclusion in the CSV file.
   b) Select whether you want all rows or your current selection of rows to be listed in the CSV file.
   c) From the available options, select the columns you want listed in the CSV file.
   d) Click **Export**.

      The CSV file is generated and available for download.

Securing Virtual Machines with AMD Secure Encrypted Virtualization-Encrypted State

Secure Encrypted Virtualization-Encrypted State (SEV-ES) is a hardware feature enabled in recent AMD CPUs that keeps the guest operating system's memory and register state encrypted, protecting it against access from the hypervisor.

You can add SEV-ES to your virtual machines as an extra security enhancement. SEV-ES prevents CPU registers from leaking information in registers to components like the hypervisor. SEV-ES can also detect malicious modifications to a CPU register state.

vSphere and AMD Secure Encrypted Virtualization-Encrypted State

In vSphere 7.0 Update 1 and later, you can activate Secure Encrypted Virtualization-Encrypted State (SEV-ES) on supported AMD CPUs and guest operating systems.

Currently, SEV-ES supports only AMD EPYC 7xx2 CPUs (code named "Rome") and later CPUs, and only versions of Linux kernels that include specific support for SEV-ES.

SEV-ES Components and Architecture

The SEV-ES architecture consists of the following components.

- AMD CPU, specifically, the Platform Security Processor (PSP) that manages encryption keys and handles encryption.
- Enlightened operating system, that is, an operating system that uses guest-initiated calls to the hypervisor.
- Virtual Machine Monitor (VMM) and Virtual Machine Executable (VMX), to initialize an encrypted virtual machine state during virtual machine power-on, and also to handle calls from the guest operating system.
- VMkernel driver, to communicate unencrypted data between the hypervisor and the guest operating system.

Implementing and Managing SEV-ES on ESXi

You must first activate SEV-ES in a system's BIOS configuration. See the documentation for your system for more information about accessing the BIOS configuration. After you have activated SEV-ES in the BIOS for your system, you can then add SEV-ES to a virtual machine.

You use either the vSphere Client (starting in vSphere 7.0 Update 2) or PowerCLI commands to activate and deactivate SEV-ES on virtual machines. You can create new virtual machines with SEV-ES, or activate SEV-ES on existing virtual machines. Privileges to manage virtual machines activated with SEV-ES are the same as for managing regular virtual machines.

Unsupported VMware Features on SEV-ES

The following features are not supported when SEV-ES is activated.

- System Management Mode
- vMotion
- Powered-on snapshots (however, no-memory snapshots are supported)
- Hot add or remove of CPU or memory
- Suspend/resume
- VMware Fault Tolerance
- Clones and instant clones
- Guest Integrity
- UEFI Secure Boot

Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine with the vSphere Client

In vSphere 7.0 Update 2 and later, you can use the vSphere Client to add SEV-ES to a virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.
- SEV-ES must be enabled in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When enabling SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.

  Note: vSphere 7.0 Update 1 supports 16 SEV-ES enabled virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES enabled virtual machines per ESXi host.
- The ESXi host running in your environment must be at ESXi 7.0 Update 1 or later.
- The vCenter Server must be at vSphere 7.0 Update 2 or later.
- The guest operating system must support SEV-ES.

  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.

- The virtual machine must have the **Reserve all guest memory** option enabled, otherwise power-on fails.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object, select **New Virtual Machine**, and follow the prompts to create a virtual machine.

Option	Action
Select a creation type	Create a virtual machine.
Select a name and folder	Specify a name and target location.
Select a compute resource	Specify an object for which you have privileges to create virtual machines.
Select storage	In the VM storage policy, select the storage policy. Select a compatible datastore.
Select compatibility	Ensure that **ESXi 7.0 and later** is selected.
Select a guest OS	Select Linux, and select a version of Linux with specific support for SEV-ES.
Customize hardware	Under **VM Options** > **Boot Options** > **Firmware**, ensure that EFI is selected. Under **VM Options** > **Encryption**, select the **Enable** check box for AMD SEV-ES.
Ready to complete	Review the information and click **Finish**.

The virtual machine is created with SEV-ES.

Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine with the vSphere Client

In vSphere 7.0 Update 2 and later, you can use the vSphere Client to add SEV-ES to an existing virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.
- SEV-ES must be activated in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When activating SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.
  Note: vSphere 7.0 Update 1 supports 16 SEV-ES activated virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES activated virtual machines per ESXi host.
- The ESXi host running in your environment must be at ESXi 7.0 Update 1 or later.
- The vCenter Server must be at vSphere 7.0 Update 2 or later.
- The guest operating system must support SEV-ES.
  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.
- The virtual machine must have the **Reserve all guest memory** option checked, otherwise power-on fails.

- Ensure that the virtual machine is powered off.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. Under **VM Options** > **Boot Options** > **Firmware**, ensure that EFI is selected.
4. In the **Edit Settings** dialog box, under **VM Options** > **Encryption**, select the **Enable** check box for AMD SEV-ES.
5. Click **OK**.

SEV-ES is added to the virtual machine.

Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine

You can add SEV-ES to a virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.
- SEV-ES must be enabled in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When enabling SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.
  Note: vSphere 7.0 Update 1 supports 16 SEV-ES enabled virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES enabled virtual machines per ESXi host.
- The ESXi host running in your environment must be at ESXi 7.0 Update 1 or later.
- The guest operating system must support SEV-ES.
  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.
- The virtual machine must have the **Reserve all guest memory** option enabled, otherwise power-on fails.
- PowerCLI 12.1.0 or later must be installed on a system with access to your environment.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator to the vCenter Server that manages the ESXi host on which you want to add a virtual machine with SEV-ES.

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. Create the virtual machine with the `New-VM` cmdlet, specifying `-SEVEnabled $true`.
   For example, first assign the host information to a variable, then create the virtual machine.

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
   ```

   If you must specify the virtual hardware version, run the `New-VM` cmdlet with the `-HardwareVersion vmx-18` parameter. For example:

   ```
   New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true -HardwareVersion vmx-18
   ```

The virtual machine is created with SEV-ES.

Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine

You can add SEV-ES to an existing virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.

- SEV-ES must be activated in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When activating SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.
  Note: vSphere 7.0 Update 1 supports 16 SEV-ES activated virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES activated virtual machines per ESXi host.
- The ESXi host running in your environment must be ESXi 7.0 Update 1 or later.
- The guest operating system must support SEV-ES.
  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.
- The virtual machine must have the **Reserve all guest memory** option checked, otherwise power-on fails.
- PowerCLI 12.1.0 or later must be installed on a system with access to your environment.
- Ensure that the virtual machine is powered off.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator to the vCenter Server that manages the ESXi host with the virtual machine to which you want to add SEV-ES.
   For example:
   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```
2. Add SEV-ES to the virtual machine with the `Set-VM` cmdlet, specifying `-SEVEnabled $true`.
   For example:
   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
   ```
   If you must specify the virtual hardware version, run the `Set-VM` cmdlet with the `-HardwareVersion vmx-18` parameter. For example:
   ```
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
   ```

SEV-ES is added to the virtual machine.

Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine with the vSphere Client

In vSphere 7.0 Update 2 and later, you can use the vSphere Client to deactivate SEV-ES on a virtual machine.

- Ensure that the virtual machine is powered off.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, under **VM Options** > **Encryption**, deselect the **Enable** check box for AMD SEV-ES.
4. Click **OK**.

SEV-ES is deactivated on the virtual machine.

Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine

You can deactivate SEV-ES on a virtual machine.

- Ensure that the virtual machine is powered off.

- PowerCLI 12.1.0 or later must be installed on a system that has access to your environment.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator to the vCenter Server that manages the ESXi host with the virtual machine from which you want to remove SEV-ES.

   For example:

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. Deactivate SEV-ES on the virtual machine with the `Set-VM` cmdlet, specifying `-SEVEnabled $false`.

   For example, first assign the host information to a variable, then deactivate SEV-ES for the virtual machine.

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
   ```

SEV-ES is deactivated on the virtual machine.

Configuring Virtual Machine Options

You can set or change virtual machine options to run VMware Tools scripts, control user access to the remote console, configure startup behavior, and more. The virtual machine options define a range of virtual machine properties, such as the virtual machine name and the virtual machine behavior with the guest operating system and VMware Tools.

Configure General Virtual Machine Options

You can set or change virtual machine options to run VMware Tools scripts, control user access to the remote console, configure startup behavior, and more. The virtual machine options define a range of virtual machine properties, such as the virtual machine name and the virtual machine behavior with the guest operating system and VMware Tools.

You can view or change virtual machine settings from the vSphere Client. Not all options are available to every virtual machine and some options rarely must change from their defaults.

The host that the virtual machine runs on and the guest operating system must support any configurations that you make.

You can view and change virtual machine settings on the **VM Options** tab of the **Edit Settings** wizard.

You can select one of the following options.

Table 166: Virtual Machine Options in the vSphere Client

Options	Description
General Options	In this section, you can view or change the following settings. • Virtual machine name • Virtual machine configuration file location • Virtual machine working location • Guest operating system and OS version Currently, you can only edit the virtual machine name. The information about the other settings is read only. To change the operating system for a VM, you have to reinstall the OS - or consider deploying a new VM with your operating system of choice.
VMware Remote Console Options	In this section, you can change the locking behavior of a virtual machine and the settings for simultaneous connections.
Encryption	In this section, you can change the encryption settings of a virtual machine.
Power Management	In this section, you can change virtual machine suspend behavior.
VMware Tools	In this section, you can change the behavior of VMware Tools scripts. You can also customize the automatic VMware Tools upgrades, automatically synchronize the guest time of the virtual machine on startup or resume with the host, and periodically synchronize the guest time with the host.

Options	Description
Virtualization Based Security	Activate or deactivate VBS for the virtual machine.
Boot Options	In this section, you can change the virtual machine boot options. For example, add a delay before booting, force entry into the BIOS or EFI setup screen, or set reboot options.
Advanced	In this section, you can change the following advanced virtual machine options. • Acceleration and logging settings • Debugging and statistics • Swap file location • Latency sensitivity
Fibre Channel NPIV	In this section, you can change the virtual node and port World Wide Names (WWNs).

General Virtual Machine Options

View or change general virtual machine settings, such as the name and location of the virtual machine, configuration file location, and operating system.

Change the Virtual Machine Name

A virtual machine must have a name that is unique within the folder where the virtual machine is located. If you move a virtual machine to a different datastore folder or host that has an existing virtual machine of the same name, you must change the virtual machine's name to keep it unique.

When you change the name of a virtual machine, you change the name used to identify the virtual machine in the vCenter Server inventory. This action does not change the name used as the computer name by the guest operating system.

The virtual machine name also determines the name of the virtual machine files and folder on the disk. For example, if you name the virtual machine win8, the virtual machine files are named win8.vmx, win8.vmdk, win8.nvram, and so on. If you change the virtual machine name, the names of the files on the datastore do not change.

Note: Migration with Storage vMotion changes the virtual machine filenames on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and .nvram files. If the new names exceed the maximum filename length, the migration does not succeed.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **General Options**.
3. Delete the existing name and enter a new name for the virtual machine in the **VM Name** text box.
4. Click **OK**.

View the Virtual Machine Configuration and Working File Location

You can view the location of the virtual machine configuration and working files. You can use this information when you configure backup systems.

Verify that the virtual machine is powered off.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click **VM Options** tab and expand **General Options**.

   The path to the location of the virtual machine configuration file appears in the **VM Config File** text box. The path to the virtual machine working location appears in the **VM Working Location** text box.

Change the Configured Guest Operating System

When you create a virtual machine, the system uses a template to specify all the parameters necessary to run the guest OS you selected so that the virtual machine can run correctly. For example, does the guest OS support hot adding devices, memory, and CPUs. After you create a virtual machine, you can add or modify various parameters. For example, you can add host bus adapters, NICs, memory sizing, storage devices, and so on.

Power off the virtual machine.

The directory where the virtual machine is stored includes a file with a .VMX extension (VMX file). The VMX file contains parameters that define and control the virtual machine.

One of the parameters in the VMX file is the guestOS parameter. This parameter does not specify the guest OS that the virtual machine uses; it determines how the low-level (implicit) parts of the virtual machine are initialized so that it can run the guest OS.

The guestOS parameter and the other parameters established through the creation template are defined and tested to ensure that the guest OS will operate adequately.

Changing the guestOS parameter is not recommended, as it can lead to undesirable results. This change only affects the guestOS parameter; no other parameters will be changed, added, or removed. The virtual machine may appear to run correctly initially, but in many cases, it will fail to power on due to incompatibilities between the guestOS parameter and other settings in the VMX file.

Note:

Do not change the guestOS parameter when the virtual machine is powered on.

You can create two virtual machines – one for the current guestOS type and one for the destination guestOS. Review the virtual machine creation templates to identify the parameters you must add, delete, or change for the virtual machine. Changing the guestOS parameter of the newly created virtual machine is the customer’s responsibility. VMware does not validate the modified virtual machine's suitability.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **General Options**.
3. From the **Guest OS** drop-down menu, select the guest operating system family.
4. From the **Guest OS Version** drop-down menu, select the guest operating system version.
5. Click **OK**.

Configuring User Mappings on Guest Operating Systems

As a vSphere administrator, you can enable guest OS access on certain SSO accounts.

Enabling SSO accounts to log in to a guest OS provides users with additional capabilities to perform administrative tasks on guest virtual machines, such as installing or upgrading the VMware Tools or configuring apps.

Functionality to allow vSphere administrators to configure a guest operating system to use VGAuth authentication. The vSphere administrator must know the guest administrator password for the enrollment process.

To enroll SSO users to a guest user account, you must enroll SSO users to accounts in guest operating systems. The enrollment process maps a vSphere user to a particular account in the guest by using SSO certificates. Subsequent guest management requests use an SSO SAML token to log in to the guest.

You must configure VMs to accept X.509 certificates. X.509 certificates allow the vSphere administrators in your data center to use SAML tokens issued by single sign-on service to access guest OSs.

View Existing SSO User Mappings

You can view the existing guest user mappings for guest operating systems on the selected virtual machine. You need to authenticate your credentials to view guest mappings.

1. Navigate to the virtual machine and click the **Configure** tab.
2. Click the **Guest User Mappings** tab.
3. To log in to your guest OS account, enter your user name and password, and click **Log In**.
   The existing in-guest user mappings are displayed.

Add SSO users to Guest Operating Systems

You can map a new SSO user to a guest user account by creating a user map. Mapping can be established for any type of SSO users, for example solution and users.

Power on the virtual machine.

1. Navigate to the virtual machine and click **Configure** tab.
2. Click the **Guest User Mappings** tab.
3. Enter your user name and password and click **Log In**.
4. In the **Guest User Mappings** pane, click the **Add** button.
   The **Add New User Mapping** dialog box opens.
5. From the list of SSO users, select the SSO user that you want to map to a guest account.
6. Specify a guest OS user name and click **OK**.
   The SSO user is mapped to a guest user account. A new guest user account is added to the list of **Guest User Mappings**.

Remove SSO Users from Guest Operating Systems

You can remove an existing SSO account from guest user mappings.

Power on your virtual machine.

1. Navigate to a virtual machine and click the **Configure** tab.
2. Click **Guest User Mappings**, enter you user name and password, and click **Log In**.
3. In the **Guest User Mappings** pane, select the SSO user from the list that you want to remove.
4. Click the **Remove** button.
5. Click **Yes** to confirm.
   The mapping between the selected SSO user account and guest OS account is removed.

VMware Remote Console Options

Change the VMware Remote Console options to control the access to the virtual machine.

Change the Virtual Machine Console Options for Remote Users

You can limit the number of simultaneous connections to a virtual machine and lock the guest operating system when the last remote user disconnects from the virtual machine console.

- Verify that VMware Tools is installed and running.

- To use the **Guest OS lock** option, verify that you have a Windows XP or later guest operating system.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab, and expand **VMware Remote Console Options**.
3. Optional: Select the **Guest OS lock** check box to lock the guest operating system when the last remote user disconnects.
4. Optional: In the **Maximum number of sessions** text box, specify the number of simultaneous connections to the virtual machine.
5. Click **OK**.

Configure Virtual Machine Encryption Options

Starting with vSphere 6.7, you can take advantage of virtual machine encryption. Encryption protects not only your virtual machine but also virtual machine disks and other files. You set up a trusted connection between vCenter Server and a key management server (KMS). vCenter Server can then retrieve keys from the KMS as needed.

For detailed information about virtual machine encryption, see the *vSphere Security* documentation.

Encrypt an Existing Virtual Machine or Virtual Disk

You can encrypt an existing virtual machine or virtual disk by changing its storage policy. You can encrypt virtual disks only for encrypted virtual machines.

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Ensure that the virtual machine is powered off.
- Verify that you have the required privileges:
  - **Cryptographic operations** > **Encrypt new**
  - If the host encryption mode is not Enabled, you also need **Cryptographic operations** > **Register host**.

This task describes how to encrypt an existing virtual machine or virtual disk using the vSphere Client.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine that you want to change and select **VM Policies** > **Edit VM Storage Policies**.

   You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.
3. Select the storage policy.
   - To encrypt the VM and its hard disks, select an encryption storage policy and click **OK**.
   - To encrypt the VM but not the virtual disks, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.

   You cannot encrypt the virtual disk of an unencrypted VM.

4. If you prefer, you can encrypt the virtual machine, or both virtual machine and disks, from the **Edit Settings** menu in the vSphere Client.
   a) Right-click the virtual machine and select **Edit Settings**.
   b) Select the **VM Options** tab, and open **Encryption**. Choose an encryption policy. If you deselect all disks, only the VM home is encrypted.
   c) Click **OK**.

Decrypt an Encrypted Virtual Machine or Virtual Disk

You can decrypt a virtual machine, its disks, or both, by changing the storage policy.

- The virtual machine must be encrypted.
- The virtual machine must be powered off or in maintenance mode.
- Required privileges: **Cryptographic operations** > **Decrypt**

This task describes how to decrypt an encrypted virtual machine using the vSphere Client.

All encrypted virtual machines require encrypted vMotion. During virtual machine decryption, the Encrypted vMotion setting remains. To change this setting so that Encrypted vMotion is no longer used, change the setting explicitly.

This task explains how to perform decryption using storage policies. For virtual disks, you can also perform decryption using the **Edit Settings** menu.

Note: In the Virtual Machine Details pane, a vTPM-enabled virtual machine displays both a lock icon and an "Encrypted with *`key_provider`*" message. To remove a vTPM from a virtual machine, see Remove Virtual Trusted Platform Module from a Virtual Machine.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine that you want to change and select **VM Policies** > **Edit VM Storage Policies**.
   You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.
3. Select a storage policy.
   - To decrypt the VM and its hard disks, toggle off **Configure per disk**, select a storage policy from the drop-down menu, and click **OK**.
   - To decrypt a virtual disk but not the virtual machine, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.

   You cannot decrypt the virtual machine and leave the disk encrypted.

4. If you prefer, you can use the vSphere Client to decrypt the virtual machine and disks from the **Edit Settings** menu.
   a) Right-click the virtual machine and select **Edit Settings**.
   b) Select the **VM Options** tab and expand **Encryption**.
   c) To decrypt the VM and its hard disks, choose **None** from the **Encrypt VM** drop-down menu.
   d) To decrypt a virtual disk but not the virtual machine, deselect the disk.
   e) Click **OK**.
5. Optional: You can change the Encrypted vMotion setting.
   a) Right-click the virtual machine and click **Edit Settings**.
   b) Click **VM Options**, and open **Encryption**.
   c) Set the **Encrypted vMotion** value.

Clone an Encrypted Virtual Machine

When you clone an encrypted virtual machine, the clone is encrypted with the same keys. To change keys for the clone, perform a recrypt of the clone using the API. For more information, see *vSphere Web Services SDK Programming Guide*.

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Required privileges:
  - **Cryptographic operations** > **Clone**
  - **Cryptographic operations** > **Encrypt**
  - **Cryptographic operations** > **Decrypt**
  - **Cryptographic operations** > **Recrypt**
  - If the host encryption mode is not `Enabled`, you also must have **Cryptographic operations** > **Register host** privilege.

You can perform the following operations during clone.

- Create an encrypted virtual machine from an unencrypted virtual machine or virtual machine template.
- Create a decrypted virtual machine from an encrypted virtual machine or virtual machine template.
- Recrypt the destination virtual machine with different keys from that of source virtual machine.

You can create an instant clone virtual machine from an encrypted virtual machine with the caveat that the instant clone shares the same key with the source virtual machine. You cannot recrypt keys on either the source or the instant clone virtual machine. See *vSphere Web Services SDK Programming Guide*.

1. Navigate to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and select **Clone** > **Clone to Virtual Machine** > .
3. Navigate through pages of the wizard.

Select a name and folder	Enter a name and select a data center or folder in which to deploy it.
Select a compute resource	Select an object for which you have privileges to create encrypted virtual machines. For information about prerequisites and required privileges for encryption tasks, see the *vSphere Security* documentation.
Select storage	Select the datastore or datastore cluster in which to store the template configuration files and all virtual disks. You can change the storage policy as part of the clone operation. For example, changing from using an encryption to non-encryption policy decrypts the disks.
Select clone options	Select additional customization options.

Ready to complete	Review and click **Finish**.

4. Optional: Change the keys for the cloned virtual machine.

   By default, the cloned virtual machine is created with the same keys as its parent. Best practice is to change the cloned virtual machine keys to ensure that multiple virtual machines do not have the same keys.

Virtual Machine Power Management Options

Configure virtual machine Power management options to define how the virtual machine responds when the guest OS is placed on standby.

Manage Power Management Settings for a Virtual Machine

If the guest operating system is placed on standby, the VM can either remain powered on or be suspended. You can use the Power Management settings to control this behavior. Some desktop-based guests, such as Windows 7, have standby enabled by default, so that the guest goes into standby after a predetermined time.

Note: To avoid having the guest operating system go into standby mode unintentionally, verify the settings before you deploy the virtual machine.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click **VM Options** and expand **Power Management**.
3. In the **Standby response** section, select the standby response of the virtual machine.
   - The **Suspend the virtual machine** option stops all processes, which saves resources, and copies the contents of the virtual machine's memory to the virtual machine's `.vmss` file. Writing the memory to the `.vmss` file is useful if you need to copy the file to help with a troubleshooting scenario.
   - The **Put the guest operating system in standby mode and leave the virtual machine powered on** option stops all processes, but leaves the virtual devices connected to the virtual machine.
4. In the **Wake on LAN** section, select one or multiple virtual network adapters to which to apply the Wake on LAN option.
5. To save your changes, click **OK**.

Configuring VMware Tools Options

Configure the VMware Tools options to define the power operations for the virtual machine and decide when to run VMware Tools Scripts. Through VMware Tools configuration, you can automatically synchronize the virtual machine guest operating system time with the host.

Configure the Virtual Machine Power States

Changing virtual machine power states is useful when you do maintenance on the host. You can use the system default settings for the virtual machine power controls, or you can configure the controls to interact with the guest operating system. For example, you can configure the **Power off** control to power off the virtual machine or shut down the guest operating system.

- Verify that you have privileges to perform the intended power operation on the virtual machine.
- To set optional power functions, install VMware Tools in the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

You can modify many virtual machine configurations while the virtual machine is running, but you might need to change the virtual machine power state for some configurations.

You cannot configure a **Power on (** **)** action. This action powers on a virtual machine when a virtual machine is stopped, or resumes the virtual machine and runs a script when it is suspended and VMware Tools is installed and available. If VMware Tools is not installed, it resumes the virtual machine and does not run a script.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **VMware Tools**.
3. Select an option for the virtual machine **Power Off** ( ) control from the drop-down menu.

Option	Description
Power Off	Immediately stops the virtual machine. The power off action shuts down the guest operating system or powers off the virtual machine. A message indicates that the guest operating system might not shut down properly. Use this power off option only when necessary.
Shut Down Guest (Default)	Follows system settings. The current value of the system settings appears in parentheses. Uses VMware Tools to initiate an orderly system shut down of the virtual machine. Soft power operations are possible only if the tools are installed in the guest operating system.

4. Select an option for the **Suspend (** **)** control from the drop-down menu.

Option	Description
Suspend (Default)	Suspends the virtual machine and leaves it connected to the network.
Suspend Guest	Follows system settings. The current value of the system setting appears in parentheses. Pauses all virtual machine activity. When VMware Tools is installed and available, the suspend action runs a script in the guest operating system and suspends the virtual machine. If VMware tools is not installed, the suspend action suspends the virtual machine without running a script.

5. Select an option for the **Reset (** **)** control from the drop-down menu.

Option	Description
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. If VMware Tools is not installed, the reset action resets the virtual machine.
Default (Restart Guest)	Follows system settings. The current value of the system setting appears in parentheses. Uses VMware Tools to initiate an orderly restart. Soft power operations are possible only if the tools are installed in the guest operating system.

6. To save your changes, click **OK**.

Synchronize the Time of a Virtual Machine Guest Operating System with the Host

You can configure VMware Tools options to set the time of a virtual machine guest operating system to be the same as the time of the host. Starting with vSphere 7.0 Update 1, VMware Tools provides accurate and synchronized time between guest and host operating systems.

To synchronize the virtual machine guest operating system time with that on the host, install VMware Tools on the virtual machine.

You can synchronize the time between guest and host operating systems while the virtual machine is running. This operation does not depend on the hardware version of the virtual machine.

For information about the timekeeping best practices for Windows guest operating systems, see https://kb.vmware.com/s/article/1318.

For information about the timekeeping best practices for Linux guest operating systems, see https://kb.vmware.com/s/article/1006427.

1. To synchronize the time of the virtual machine guest operating system with the host time, open VMware Tools options for your virtual machine while creating, editing, cloning or deploying a virtual machine.

Option	Action
Create a virtual machine	1. Right-click any inventory object that is a valid parent object of a virtual machine and select **New Virtual Machine**. 2. On the **Select a creation type** page, select **Create a new virtual machine** and click **Next**. 3. Navigate through the pages of the wizard. 4. On the **Customize hardware** page, click the **VM Options** tab and expand **VMware Tools**.
Edit a virtual machine	1. Right-click a virtual machine in the inventory and select **Edit Settings**. 2. Click the **VM Options** tab and expand **VMware Tools**.
Clone an existing virtual machine	1. Right-click a virtual machine in the inventory and select **Clone** > **Clone to Virtual Machine**. 2. Navigate through the pages of the wizard. 3. On the **Select clone options** page, select **Customize this virtual machine's hardware** and click **Next**. 4. On the **Customize hardware** page, click the **VM Options** tab and expand **VMware Tools**.
Deploy a virtual machine from a template	1. Right-click a template in the inventory and select **New VM from This Template**. 2. Navigate through the pages of the wizard. 3. On the **Select clone options** page, select **Customize this virtual machine's hardware** and click **Next**. 4. On the **Customize hardware** page, click the **VM Options** tab and expand **VMware Tools**.

2. Select the time synchronization options.

Option	Action
Synchronize at startup and resume (Default)	This option is selected by default to ensure the best time synchronization between guest and host operating systems after performing certain operations, for example: • When you resume a virtual machine from a suspended operation. • When you migrate a virtual machine with vMotion. • When you revert a snapshot.
Synchronize time periodically	Periodically synchronize the time of the guest operating system of a virtual machine with the host. **Note:** Select this option if the guest operating system of a virtual machine does not have a native time synchronization software.

3. To save your changes, click **OK**.

Virtualization Based Security

Microsoft VBS, a feature of Windows 10 and Windows Server 2016 operating systems, uses hardware and software virtualization to enhance system security by creating an isolated, hypervisor-restricted, specialized subsystem. Starting

with vSphere 6.7, you can enable Microsoft virtualization-based security (VBS) on supported Windows guest operating systems.

For more detailed information about VBS, see the *vSphere Security* documentation.

Enable Virtualization-based Security on an Existing Virtual Machine

You can enable Microsoft virtualization-based security (VBS) on existing virtual machines for supported Windows guest operating systems.

Using Intel CPUs for VBS requires vSphere 6.7 or later. The virtual machine must have been created using hardware version 14 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit) or later releases
- Windows Server 2016 (64 bit) or later releases

Using AMD CPUs for VBS requires vSphere 7.0 Update 2 or later. The virtual machine must have been created using hardware version 19 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit), version 1809 or later releases
- Windows Server 2019 (64 bit) or later releases

Ensure that you install the latest patches for Windows 10, version 1809, and Windows Server 2019, before enabling VBS.

For more information about activating VBS on virtual machines on AMD platforms, see the VMware KB article at https://kb.vmware.com/s/article/89880.

Enabling VBS is a process that involves first enabling VBS in the virtual machine then enabling VBS in the guest OS.

Note: New virtual machines configured for Windows 10, Windows Server 2016, and Windows Server 2019 on hardware versions less than version 14 are created using Legacy BIOS by default. If you change the virtual machine's firmware type from Legacy BIOS to UEFI, you must reinstall the guest operating system.

1. In the vSphere Client, browse to the virtual machine.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click the **VM Options** tab.
4. Select the **Enable** check box for Virtualization Based Security.
5. Click **OK**.

Confirm that the virtual machine's **Summary** tab displays "VBS true" in the Guest OS description.

See Enable Virtualization-based Security on the Guest Operating System.

Enable Virtualization-based Security on the Guest Operating System

You can enable Microsoft virtualization-based security (VBS) for supported Windows guest operating systems.

- Ensure that virtualization-based security has been enabled on the virtual machine.

You enable VBS from within the Windows Guest OS. Windows configures and enforces VBS through a Group Policy Object (GPO). The GPO gives you the ability to turn off and on the various services, such as Secure Boot, Device Guard, and Credential Guard, that VBS offers. Certain Windows versions also require you to perform the additional step of enabling the Hyper-V platform.

See Microsoft's documentation about deploying Device Guard to enable virtualization-based security for details.

1. In Microsoft Windows, edit the group policy to turn on VBS and choose other VBS-related security options.
2. Optional: For Microsoft Windows versions less than Redstone 4, in the Windows Features control panel, enable the Hyper-V platform.
3. Reboot the guest operating system.

Deactivate Virtualization-based Security

If you no longer use virtualization-based security (VBS) with a virtual machine, you can deactivate VBS. When you deactivate VBS for the virtual machine, the Windows VBS options remain unchanged but might induce performance issues. Before deactivating VBS on the virtual machine, deactivate VBS options within Windows.

Ensure that the virtual machine is powered off.

1. In the vSphere Client, browse to the virtual machine that is using VBS.
   See Identify VBS-Enabled Virtual Machines for help in locating virtual machines that use VBS.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click **VM Options**.
4. Deselect the **Enable** check box for Virtualization Based Security.
   A message reminds you to deactivate VBS in the guest OS.
5. Click **OK**.
6. Verify that the virtual machine's **Summary** tab no longer displays "VBS true" in the Guest OS description.

Identify VBS-Enabled Virtual Machines

You can identify which of your virtual machines have VBS enabled, for reporting and compliance purposes.

1. Connect to vCenter Server by using the vSphere Client.
2. Select a vCenter Server instance, a data center, or a host in the inventory.
3. Click the **VMs** tab and click **Virtual Machines**.
4. In the list of virtual machines, click the down arrow in a column header to show/hide columns, and select the **VBS** check box.
   The **VBS** column appears.
5. Scan for Present in the **VBS** column.

Configure Virtual Machine Boot Options

Edit Boot Options to activate or deactivate UEFI Secure Boot and configure the boot behavior of the virtual machine.

Activate or Deactivate UEFI Secure Boot for a Virtual Machine

UEFI Secure Boot is a security standard that helps ensure that your PC boots using only software that is trusted by the PC manufacturer. For certain virtual machine hardware versions and operating systems, you can activate secure boot just as you can for a physical machine.

You can activate secure boot only if all prerequisites are met. If prerequisites are not met, the check box is not visible in the vSphere Client.

- Verify that the virtual machine operating system and firmware support UEFI boot.
  - EFI firmware
  - Virtual hardware version 13 or later.
  - Operating system that supports UEFI secure boot.

  Note: Some guest operating systems do not support changing from BIOS boot to UEFI boot without guest OS modifications. Consult your guest OS documentation before changing to UEFI boot. If you upgrade a virtual machine that already uses UEFI boot to an operating system that supports UEFI secure boot, you can activate Secure Boot for that virtual machine.
- Turn off the virtual machine. If the virtual machine is running, the check box is dimmed.

In an operating system that supports UEFI secure boot, each piece of boot software is signed, including the bootloader, the operating system kernel, and operating system drivers. The virtual machine's default configuration includes several code signing certificates.

- A Microsoft certificate that is used only for booting Windows.
- A Microsoft certificate that is used for third-party code that is signed by Microsoft, such as Linux bootloaders.
- A VMware certificate that is used only for booting ESXi inside a virtual machine.

The virtual machine's default configuration includes one certificate for authenticating requests to modify the secure boot configuration, including the secure boot revocation list, from inside the virtual machine, which is a Microsoft KEK (Key Exchange Key) certificate.

In almost all cases, it is not necessary to replace the existing certificates. If you do want to replace the certificates, see the VMware Knowledge Base system.

VMware Tools version 10.1 or later is required for virtual machines that use UEFI secure boot. You can upgrade those virtual machines to a later version of VMware Tools when it becomes available.

For Linux virtual machines, VMware Host-Guest Filesystem is not supported in secure boot mode. Remove VMware Host-Guest Filesystem from VMware Tools before you activate secure boot.

Note: If you turn on secure boot for a virtual machine, you can load only signed drivers into that virtual machine.

This task describes how to use the vSphere Client to activate and deactivate secure boot for a virtual machine. You can also write scripts to manage virtual machine settings. For example, you can automate changing the firmware from BIOS to EFI for virtual machines with the following PowerCLI code:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

See *VMware PowerCLI User's Guide* for more information.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click the **VM Options** tab, and expand **Boot Options**.
4. Under **Boot Options**, ensure that firmware is set to **EFI**.
5. Select your task.
   - Select the **Secure Boot** check box to activate secure boot.
   - Deselect the **Secure Boot** check box to deactivate secure boot.

6. Click **OK**.

When the virtual machine boots, only components with valid signatures are allowed. The boot process stops with an error if it encounters a component with a missing or invalid signature.

Delay the Boot Sequence

Delaying the boot operation is useful when you change BIOS or EFI settings such as the boot order. For example, you can change the BIOS or EFI settings to force a virtual machine to boot from a CD-ROM.

- Verify that vSphere Client is logged in to a vCenter Server.
- Verify that you have access to at least one virtual machine in the inventory.
- Verify that you have privileges to edit boot options for the virtual machine.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click **VM Options** tab and expand **Boot Options**.
3. In the **Boot Delay** section, select the time in milliseconds to delay the boot operation.
4. Optional: In the **Force setup** section, select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots.
5. Optional: In the **Failed Boot Recovery** section, select whether the virtual machine should reboot after a boot failure and enter the time in seconds.
6. Click **OK**.

Configuring Virtual Machine Advanced Options

You can edit the Advanced virtual machines settings when you need to solve issues caused by an application or when you need log files and debugging information for troubleshooting purposes. You can also add or change configuration parameters and change the latency sensitivity of a virtual machine.

Deactivating Virtual Machine Acceleration

When you install or run software in a virtual machine, the virtual machine appears to stop responding. The problem occurs early when you run an application. You can resolve the issue by temporarily deactivating acceleration in the virtual machine.

The **Disable acceleration** option slows down virtual machine performance, so use it only to solve the issue caused by running the application. After the application stops encountering problems, deselect **Disable acceleration**. You might be able to run the application with acceleration.

You can enable and deactivate acceleration when the virtual machine is running.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Advanced**.
3. Select **Disable acceleration**.
4. Click **OK**.

You can install or run the software successfully.

Enable Virtual Machine Logging

You can enable logging to collect log files to help troubleshoot problems with your virtual machine.

Required privilege: **Virtual machine** > **Configuration** > **Settings**

ESXi hosts store virtual machine log files in the same directory as the virtual machine's configuration files. By default, the log file name is `vmware.log`. Archived log files are stored as `vmware-n.log` , where *n* is a number in sequential order beginning with 1.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Advanced**.
3. In the Settings row, select **Enable logging** and click **OK**.

You can view and compare log files in the same storage location as the virtual machine configuration files.

Configure Virtual Machine Debugging and Statistics

You can run a virtual machine so that it collects additional debugging information that is helpful to VMware technical support in resolving issues.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Advanced**.
3. Select a debugging and statistics option from the drop-down menu.
   - **Run normally**
   - **Record Debugging Information**
   - **Record Statistics**
   - **Record Statistics and Debugging Information**

   The number of debugging and statistics options available depends on the host software type and version. On some hosts, some options are not available.
4. Click **OK**.

Change the Swap File Location

When a virtual machine is powered on, the system creates a VMkernel swap file to serve as a backing store for the virtual machine's RAM contents. You can accept the default swap file location or save the file to a different location. By default, the swap file is stored in the same location as the virtual machine's configuration file.

Power off the virtual machine.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Advanced**.
3. Select a swap file location option.

Option	Description
Default	Stores the virtual machine swap file at the default location defined by the host or cluster swap file settings.
Virtual machine directory	Stores the virtual machine swap file in the same folder as the virtual machine configuration file.
Datastore specified by host	If the host or cluster settings define a location for the swap file, this location is used. Otherwise, the swap file is stored with the virtual machine.

4. Click **OK**.

Edit Configuration File Parameters

You can change or add virtual machine configuration parameters when instructed by a VMware technical support representative, or if you see VMware documentation that instructs you to add or change a parameter to fix a problem with your system.

Important: Changing or adding parameters when a system does not have problems might lead to decreased system performance and instability.

The following conditions apply:

- To change a parameter, you change the existing value for the keyword/value pair. For example, if you start with the keyword/value pair, keyword/value, and change it to keyword/value2, the result is keyword=value2.
- You cannot delete a configuration parameter entry.

CAUTION: You must assign a value to configuration parameter keywords. If you do not assign a value, the keyword can return a value of 0 or false, which can result in a virtual machine that cannot power on.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Advanced**.
3. Click **Edit Configuration**.
4. Optional: To add a parameter, click **Add Configuration Parameters** and type a name and value for the parameter.
5. Optional: To change a parameter, type a new value in the **Value** text box for that parameter.
6. Click **OK**.

Configure Fibre Channel NPIV Settings

N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers. This capability lets you control virtual machine access to LUNs on a per-virtual machine basis.

- To edit the virtual machine's WWNs, power off the virtual machine.
- Verify that the virtual machine has a datastore containing a LUN that is available to the host.

Each virtual port is identified by a pair of world wide names (WWNs) that vCenter Server assigns. The pair consists of a world wide port name (WWPN) and a world wide node name (WWNN).

For detailed information on how to configure NPIV for a virtual machine, see the *vSphere Storage* documentation.

NPIV support is subject to the following limitations:

- NPIV must be enabled on the SAN switch. Contact the switch vendor for information about enabling NPIV on their devices.
- NPIV is supported only for virtual machines with RDM disks. Virtual machines with regular virtual disks continue to use the WWNs of the host's physical HBAs.
- The physical HBAs on the ESXi host must have access to a LUN though their WWNs in order for the virtual machines on that host to have access to that LUN using their NPIV WWNs. Ensure that access is provided to both the host and the virtual machines.
- The physical HBAs on the ESXi host must support NPIV. If the physical HBAs do not support NPIV, the virtual machines on that host start using the WWNs of the physical HBAs for LUN access.

- Each virtual machine can have up to 4 virtual ports. NPIV-enabled virtual machines are assigned exactly 4 NPIV-related WWNs, which are used to communicate with physical HBAs through virtual ports. Therefore, virtual machines can use up to 4 physical HBAs for NPIV purposes.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Fibre Channel NPIV**.
3. Optional: Select the **Temporarily Disable NPIV for this virtual machine** check box.
4. Select an option for assigning WWNs.
   - To leave WWNs unchanged, select **Leave unchanged**.
   - To have vCenter Server or the ESXi host generate new WWNs, select **Generate New WWNs**.
   - To remove the current WWN assignments, select **Remove WWN assignment**.
5. Click **OK**.

Managing Multi-Tiered Applications with vSphere vApp

With vSphere vApp, you can package multiple interoperating virtual machines and software applications into a single unit that you can manage and distribute in OVF format.

A vApp can contain one or more virtual machines. Any operation carried out with the vApp, such as clone or power off, affects all virtual machines in the vApp container.

In the vSphere Client, you can navigate to the vApp **Summary** tab, where you can view the current status of the vApp, and you can manage the vApp.

Note: Because the vApp metadata resides in the vCenter Server database, a vApp can be distributed across multiple ESXi hosts. The metadata information might be lost if the vCenter Server database is cleared or if the standalone ESXi host that contains the vApp is removed from the vCenter Server. Back up your vApps to an OVF package to avoid losing metadata.

vApp metadata for the virtual machines within the vApp does not follow the snapshot semantics for virtual machine configuration. The vApp properties that you delete, modify, or define after you take a snapshot of a virtual machine remain respectively deleted, modified, or defined, if the virtual machine reverts to that snapshot or any prior snapshots.

Create a vApp

A vApp allows you to perform resource management and certain other management activities such as power operations for multiple virtual machines at the same time. You can think of the vApp as the container for the virtual machines, and you can perform the operations on the container.

Verify that one of those objects is available in your data center.

- A standalone host that is running ESX 4.0 or later
- A DRS cluster

When you create a vApp, you can add it to a folder, standalone host, resource pool, DRS cluster, or another vApp.

1. In the vSphere Client, right-click an object that supports vApp creation and click **New vApp**.

   The **New vApp** wizard starts.
2. On the **Select creation type** page, select **Create a new vApp** and click **Next**.
3. On the **Select a name and location** page, type a name and select a location for the vApp, and click **Next**.
   - If you start the creation process from a folder or vApp, you are prompted for a host, cluster, or resource pool.
   - If you start the creation process from a resource pool, host, or cluster, you are prompted for a folder or a data center.

4. On the Resource allocation page, allocate CPU and memory resources to the vApp.

Option	Description
Shares	Defines the CPU or memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares that expresses a proportional weight.
Reservation	Defines the guaranteed CPU or memory allocation for this vApp.
Reservation Type	Defines whether the reservation is expandable. Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Defines the upper limit for this vApp's CPU or memory allocation. Select **Unlimited** to specify no upper limit.

5. On the **Review and finish** page, review the vApp settings and click **Finish**.

Perform vApp Power Operations

One of the advantages of a vApp is that you can perform power operations on all virtual machines it contains at the same time.

When powering on a vApp within a DRS cluster in manual mode, no DRS recommendations are generated for virtual machine placements. The power-on operation performs as if DRS is run in a semiautomatic or automatic mode for the initial placements of the virtual machines. This does not affect vMotion recommendations. Recommendations for individual powering on and powering off of virtual machines are also generated for vApps that are running.

1. Navigate to a vApp in the inventory.
2. Select one of the power operation options.

Task	Action
Power on	Right-click the vApp and select **Power** > **Power On**. You can power on a vApp to power on all its virtual machines and child vApps. Virtual machines are powered on according to the startup order configuration. If a delay is set in the startup settings of a virtual machine in the vApp, the vApp waits for the set length of time before powering on that virtual machine.
Power off	Right-click the vApp and select **Power** > **Power Off** You can power off a vApp to power off all its virtual machines and child vApps. Virtual machines are powered off in reverse startup order. If a delay is set in the shutdown settings of a virtual machine in the vApp, the vApp waits for the set length of time before powering off that virtual machine.
Suspend	Right-click the vApp and select **Power** > **Suspend**. You can suspend a vApp to suspend all its virtual machines and child vApps. Virtual machines are suspended in the reverse order of the specified startup order. All virtual machines are suspended regardless of the Suspend behavior you specified in the Power Management VM Option for the virtual machine.

Task	Action
Resume	Right-click a vApp that is powered off or suspended and select **Power On**. Virtual machines are resumed according to their startup order configuration.

On the **Summary** tab, the **Status** indicates the vApp status.

Create or Add an Object to a vApp

You can populate a vApp with objects by creating a new virtual machine, resource pool, or child vApp within the vApp. Alternatively, you can add an existing object from the inventory, such as a virtual machine or another vApp, to the vApp.

Select your task.

- Create an object inside a vApp.
  - Right-click a vApp in the inventory, and select **New Virtual Machine** to create a new virtual machine within the vApp.
  - Right-click a vApp in the inventory, and select **New Child vApp** to create a child vApp inside the vApp.
  - Right-click a vApp in the inventory, and select **New Resource Pool** to create a new resource pool within the vApp.
  - Right-click a vApp in the inventory, and select **Deploy OVF Template** to deploy an OVF template and add the corresponding virtual machine to the selected vApp.
- Add an existing object to a vApp.
  a. Navigate to an object in the inventory.
  b. Drag the object to the destination vApp.
  c. Release the mouse button.
     If the move is not permitted, the object is not added to the vApp.

The new object is now a part of the vApp in the vApp inventory.

Clone a vApp

Cloning a vApp is similar to cloning a virtual machine. When you clone a vApp, you clone all virtual machines and vApps within the vApp.

When you clone a vApp, you can add the clone to a folder, standalone host, resource pool, cluster enabled for DRS, or another vApp.
Verify that one of those objects is available in your datacenter.

- A standalone host that runs ESXi 3.0 or later
- A DRS cluster

1. Start the cloning wizard.
   - Start the cloning wizard from a DRS cluster by right-clicking the cluster and selecting **New vApp** > **New vApp** ( ).
   - Start the cloning wizard from an existing vApp by right-clicking the vApp and selecting **Clone** > **Clone**.
2. On the Select creation type page, select **Clone an existing vApp** and click **Next**.
3. On the Select source vApp page, select an existing vApp to clone, and click **Next**.
   The Select source vApp page appears only if you start the wizard from a DRS cluster.

4. On the Select destination page, select a valid host, vApp, or resource pool in which to run the vApp, and click **Next**.
5. On the Select a name and location page, type a name for the vApp, select location, and click **Next**.
6. On the Select storage page, select the virtual disk format and the target datastore and click **Next**.
7. On the Map networks page, configure the network mappings for the networks that the virtual machines in the vApp use.
8. On the Resource allocation page, allocate CPU and memory resources for the vApp and click **Next**.
9. On the Review and finish page, review the vApp settings and click **Finish**.

Edit vApp Notes

You can add or edit notes for a particular vApp.

1. Right-click a vApp in the inventory and select **Edit Notes**.
2. Type your comments in the **Edit Notes** window.
3. Click **OK**.

Your comments appear on the **Summary** tab for the vApp.

Configure vApp Properties

Define and use custom properties to present custom information to all the virtual machines in the vApp. You can later on assign values and edit those properties. If you deployed the vApp from an OVF file, and properties were predefined in that OVF, you can edit those properties as well.

- Power off the vApp.
- Required privilege: **vApp** > **vApp application configuration** on the vApp.

The **Properties** pane contains a list of all the properties that are defined for a vApp. You can use the filters to browse through the list more easily.

1. Navigate to a vApp in the inventory.
2. On the **Configure** tab, select **Settings** > **vApp properties**.
   The **Properties** pane shows the list of properties and the permissible actions.
3. Select your task by clicking the respective button.

Option	Description
Add	Creates a new property. **Important:** If the virtual machine is connected to a distributed switch and has the vApp option enabled, you cannot select any of the following **Dynamic property** options: IP address, Subnet, Netmask, Gateway, Domain name, HTTP Proxy, Host prefix, DNS servers, DNS search path, Network name.
Edit	Edits the property. You can change the general information for the property, such as the property label, category and description. You can also edit the type parameters. **Important:** If the virtual machine is connected to a distributed switch and has the vApp option enabled, you cannot select any of the following **Dynamic property** options: IP address, Subnet, Netmask, Gateway, Domain name, HTTP Proxy, Host prefix, DNS servers, DNS search path, Network name.

Option	Description
Set Value	Sets a value for the property. That value is different from the default value that you define when you create a new property.
Delete	Removes a property from the list.

Edit vApp Settings

You can edit and configure several vApp settings, including startup order, resources, and custom properties.

1. Right-click a vApp in the inventory and click **Edit Settings**.
2. On the **Resources** tab, edit CPU and memory settings, such as shares, reservation, and limit.
3. On the **Start Order** tab, set and edit the start order of the virtual machines.
4. On the **IP Allocation** tab, specify IP protocol and choose an IP allocation scheme.
5. On the **Details** tab, view product information, such as name, vendor, product URL, and vendor URL.

Configure vApp CPU and Memory Resources

You can configure the CPU and memory resource allocation for the vApp.

Reservations on vApps and all their child resource pools, child vApps, and child virtual machines count against the parent resources only if those objects are powered on.

1. Right-click a vApp in the inventory and click **Edit Settings**.
2. To allocate CPU resources to the vApp, click the **Resources** tab and expand **CPU**.

Option	Description
Shares	CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed CPU allocation for this vApp.
Reservation Type	To make the reservation expandable, select the **Expandable** check box. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's CPU allocation. Select **Unlimited** to specify no upper limit.

3. To allocate memory resources to the vApp, click the **Resources** tab and expand **Memory**.

Option	Description
Shares	Memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed memory allocation for this vApp.
Reservation Type	To make the reservation expandable, select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's memory allocation. Select **Unlimited** to specify no upper limit.

4. Click **OK**.

Configure vApp IP Allocation Policy

If your vApp is set up to allow it, and if you have the required privileges, you can edit how IP addresses are allocated for the vApp.

Required privilege:**vApp** > **vApp instance configuration**

You cannot configure the IP allocation policy during the vApp creation process.

Before you configure the IP allocation policy, you must specify the IP protocol and the IP allocation scheme that the vApp supports.

If you deploy a vApp from an OVF template, the IP allocation policy might still be editable.

1. Right-click a vApp in the inventory and click **Edit Settings**.
2. In the **Edit vApp** dialogue box, click the **IP Allocation** tab.
   This tab is only available in the vSphere Client.
3. In the Authoring section, define the IP protocol and the IP allocation scheme that the vApp supports.

   The IP protocol and the IP allocation scheme determine what options for IP allocation are available.

   A vApp can obtain its network configuration through the OVF environment or through a DHCP server. If you do not select any of these options, the IP addresses are manually allocated.

   The IP protocols that a vApp can support are IPv4, IPv6, or both.
4. In the Deployment section, select an IP allocation policy from the **IP allocation** drop-down menu.

Option	Description
Static - Manual	IP addresses are manually configured. No automatic allocation is performed.
Transient - IP Pool	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off.

   Static - IP Pool and Transient - IP Pool have in common that IP allocation is done through the range managed by the vSphere platform as specified by the IP pool range in a network protocol profile. The difference is that for a static IP Pool, the IP addresses are allocated at first power-on and remain allocated, while for a transient IP Pool, the IP addresses are allocated when needed, typically at power-on, but released during power-off.
5. Click **OK**.

Configure vApp Startup and Shutdown Options

You can change the order in which virtual machines and nested vApps within a vApp start up and shut down. You can also specify the delays and actions performed at startup and shutdown.

1. Right-click a vApp in the inventory and click **Edit Settings**.
2. Select a virtual machine and select its order group.

   Virtual machines and vApps in the same group are started before the objects in the next group. The first group of virtual machines to power on is Group 1, followed by Group 2, Group 3, and so forth. The reverse order is used for shutdown.

3. Click the **Start Order** tab and select a virtual machine from the list.
4. From the **Group** drop-down menu, select a group for the virtual machine.
5. Optional: Select the startup action for the virtual machine.
   The default is **Power On**. Select **None** to power on the virtual machine manually.
6. Optional: Specify when the startup action is to happen.
   - Enter a time delay in seconds for the startup action.
   - To perform the startup action when VMware Tools has started, select **Continue when VMware Tools are ready**.
7. Optional: Select the shutdown action for the virtual machine.
   The default shutdown action is **Power Off**. You can also select **Guest Shutdown** to shut down the guest OS and leave the virtual machine running, **Suspend**, or **None**.
8. Optional: Enter a time delay in seconds for the shutdown action.
9. Click **OK**.

Configure vApp Product Properties

You can configure product and vendor information for a vApp.

Required privilege:**vApp** > **vApp application configuration** on the vApp.

1. Right-click a vApp in the inventory and click **Edit Settings**.
2. To enter product and vendor information, click the **Details** tab.

vApp Setting	Description
Name	Product name.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.
Vendor	Vendor name.
Vendor URL	If you enter a vendor URL, a user can click the vendor name from the **Summary** page of the virtual machine and go to the vendor's web page.

3. Click **OK**.

View vApp License Agreements

You can view the license agreement for the vApp that you edit.

1. Navigate to a vApp in the inventory.
2. On the **Configure** tab, expand **Settings** and click **License agreements**.

Add a Network Protocol Profile

A network protocol profile contains a pool of IPv4 and IPv6 addresses. vCenter Server assigns those resources to vApps or to the virtual machines with vApp functionality that are connected to the port groups associated with the profile.

You can configure network protocol profile ranges for IPv4, IPv6, or both. vCenter Server uses these ranges to dynamically allocate IP addresses to the virtual machines within a vApp, when the vApp uses transient IP allocation policy.

Network protocol profiles also contain settings for the IP subnet, the DNS, and HTTP proxy servers.

Note: If you move a vApp or a virtual machine that retrieves its network settings from a protocol profile to another data center, to power on the vApp or virtual machine you must assign a protocol profile to the connected port group on the destination data center.

1. Navigate to a data center that is associated with a vApp.
2. On the **Configure** tab, select **More** > **Network Protocol Profiles**.

   Existing network protocol profiles are listed.
3. Click the **Add** button.

   The **Add Network Protocol Profile** wizard opens.
4. On the **Name and network** page, enter the name of the network protocol profile and select the networks that use this profile. Click **Next**.

   A network can be associated with one network protocol profile at a time.

5. On the **IPv4** page, configure the relevant IPv4 settings.
   a) In the **Subnet** and the **Gateway** text boxes, enter the IP subnet and gateway.
   b) To indicate that the DHCP server is available on the network, select the **DHCP Present** radio button.
   c) In the **DNS server addresses** text box, enter the DNS server information.
   d) To specify an IP pool range, enable the **IP Pool** option.
   e) If you enable IP pools, enter a comma-separated list of host address ranges in the **IP pool range** text box.

      A range consists of an IP address, a pound sign (#), and a number indicating the length of the range.

      For example, `10.20.60.4#10, 10.20.61.0#2` indicates that the IPv4 addresses can range from 10.20.60.4 to 10.20.60.13 and 10.20.61.0 to 10.20.61.1.

      The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** text box cannot include the gateway address.
   f) Click **Next**.
6. On the **IPv6** page, configure the relevant IPv6 settings.
   a) In the **Subnet** and the **Gateway** text boxes, enter the IP subnet and gateway.
   b) Select the **DHCP Present** radio button to indicate that the DHCP server is available on this network.
   c) In the **DNS server addresses**, enter the DNS server information.
   d) Enable the **IP Pool** option to specify an IP pool range.
   e) If you enable IP pools, enter a comma-separated list of host address ranges in the **IP pool range** text box.

      A range consists of an IP address, a pound sign (#), and a number indicating the length of the range.

      For example, assume that you specify the following IP pool range: `fe80:0:0:0:2bff:fe59:5a:2b#10, fe80:0:0:0:2bff:fe59:5f:b1#2`. Then the addresses are in this range:

      fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

      and

      fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2 .

      The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** text box cannot include the gateway address.
   f) Click **Next**.
7. On the **Other network configurations** page, specify additional network configurations.
   a) Enter the DNS domain.
   b) Enter the host prefix.
   c) Enter the DNS search path.

      The search paths are specified as a list of DNS domains separated by commas, semi-colons, or spaces.
   d) Enter the server name and port number for the proxy server.

      The server name must include a colon and a port number. For example, `web-proxy:3912` is a valid proxy server.
   e) Click **Next**.
8. On the **Name and Network Assignment** page, review the settings and click **Finish**.

Assign a Port Group or Network to a Network Protocol Profile

In the vSphere Client, to apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, assign the network or distributed port group that controls the networking of the virtual machine to the network protocol profile.

1. Navigate to a data center that is associated with a vApp.
2. On the **Configure** tab, select **More** > **Network Protocol Profiles**.
   Existing network protocol profiles are listed.
3. Select a nework protocol profile from the list and click the **Assign** button.
   The **Assign Networks** dialog box opens.
4. Select a port group or a network to assign to the network protocol profile.
   - On the **Distributed portgroups** tab, you see a list of the distributed port groups.
   - On the **Networks** tab, you see a list of the port groups of standard switches.

   You can select multiply port groups before you close the dialog box.
5. Click **Save**.

The port groups that you selected are now associated with the network protocol profile.

To apply to a virtual machine or vApp the range of IP addresses that the network protocol profile contains, configure the virtual machine or vApp to use the network protocol profile. For more information, see Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp .

Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp

After you associate a network protocol profile with a port group of a standard switch or a distributed switch, you can use the profile to dynamically allocate IP addresses to a virtual machine that is within a vApp.

Verify that the virtual machine is connected to a port group that is associated with the network protocol profile.

Select your task.

Option	Description
Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine	1. Navigate to a virtual machine in the vCenter Server inventory. 2. On the **Configure tab**, expand **Settings** and select **vApp Options**. 3. Click the **Edit** button. The **Edit vApp options** dialog box opens. 4. If vApp options are not enabled, select the **Enable vApp options** check box. 5. Click the **IP Allocation** tab. 6. In the Authoring section, select **OVF environment** as an IP allocation scheme. 7. In the Deployment section, set the **IP allocation** to **Transient - IP Pool** or **Static - IP Pool**. 8. Click **OK**.
Use a Network Protocol Profile to Allocate IP Addresses to a vApp	1. Navigate to a vApp in the vCenter Server inventory 2. Right-click the vApp and select **Edit Settings**. The **Edit vApp** dialog box opens. 3. Click the **IP Allocation** tab. 4. In the Authoring section, select **OVF environment** as an IP allocation scheme. 5. In the Deployment section, set the **IP allocation** to **Transient - IP Pool** or **Static - IP Pool**. 6. Click **OK**.

Both the **Static - IP Pool** and **Transient - IP Pool** options allocate an IP address from the range defined in the network protocol profile that is associated with the port group. If you select **Static - IP Pool**, the IP address is assigned the first time the virtual machine or vApp is powered on. The assigned IP address persists across restarts. If you select **Transient - IP Pool**, an IP address is assigned every the virtual machine or vApp is powered on.

When the virtual machine is powered on, the adapters connected to the port group receive IP addresses from the range in the protocol profile. When the virtual machine is powered off, the IP addresses are released.

Virtual Machine vApp Options

You can enable and configure vApp functionality for virtual machines that are not within a vApp. When a virtual machine vApp options are enabled, you can configure OVF properties, use the OVF environment, and specify IP allocation and product information for the virtual machine.

You can configure and modify the authoring vApp options of a virtual machine to specify custom information that is preserved and used when you export the virtual machine as an OVF template. If you later deploy that OVF template, the information that you specified is available for editing in the deployment vApp options of the virtual machine.

For a virtual machine with vApp options enabled, the authoring vApp options are preserved when you export the virtual machine as an OVF template and those options are used when you deploy a new virtual machine from that template. Deployment vApp options are available for virtual machines that are deployed from OVF templates.

Activate vApp Options for a Virtual Machine

To activate the vApp functionality for a virtual machine that is not part of a vApp, you must enable vApp options at the virtual machine level. Virtual machine vApp options are saved when you export the virtual machine as an OVF template. Those vApp options are later used when you deploy the OVF template.

If you activate vApp options and export a virtual machine to OVF, the virtual machine receives an OVF Environment XML descriptor at boot time. The OVF descriptor might include values for custom properties, including network configuration and IP addresses.

The OVF environment can be transported to the guest in two ways:

- As a CD-ROM that contains the XML document. The CD-ROM is mounted on the CD-ROM drive.
- Through VMware Tools. The guest OS environment variable `guestinfo.ovfEnv` contains the XML document.

For information on how to create a vApp, see Create a vApp.

1. Navigate to a virtual machine from the vCenter Server inventory.
2. On the **Configure** tab, expand **Settings** and select **vApp options**.
3. Click the **Edit** button.
   The **Edit vApp Options** dialog box opens.
4. If vApp options are deactivated, select the **Enable vApp options** check box and click **OK**.

Edit Application Properties and OVF Deployment Options for a Virtual Machine

If a virtual machine is a deployed OVF template, you can view the application properties and the OVF deployment options that are defined in the OVF. The deployment options include information about unrecognized OVF sections and the IP allocation policy.

Verify that the virtual machine has the vApp options enabled. See Activate vApp Options for a Virtual Machine.

1. Navigate to a virtual machine from the vCenter Server inventory.
2. On the **Configure** tab, expand **Settings** and select **vApp options**.
3. Click the **Edit** button.
   The **Edit vApp Options** dialog box opens.
4. If the OVF template included editable IP allocation options, click the **IP Allocation** tab and modify the IP allocation options in the **Deployment** section.

Option	Description
Static - Manual	IP addresses are manually configured. No automatic allocation is performed.
Transient - IP Pool	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off.

   With the **Static - IP Pool** and **Transient - IP Pool** options, the allocation of IP addresses is done through an IP pool range defined in a network protocol profile. The difference between the two options is that with a static IP pool, the IP addresses are allocated at the first power on of the virtual machine and remain allocated, while with a transient IP pool, the IP addresses are allocated when needed, typically at power-on, and released during power-off.

OVF Authoring Options for a Virtual Machine

You can use the OVF authoring options that are included in a virtual machine's vApp options to specify custom information that is preserved when you export the virtual machine as an OVF template.

vApp properties are a central concept to vApp deployment and self-configuration. They can turn a general OVF package into a running vApp instance with a custom configuration.

The set of properties assigned to a running vApp is determined by the OVF package from which the vApp is deployed.

- When an OVF package is created the author adds the set of properties necessary for the vApp to function in an unknown environment. For example, properties that contain network configuration, a property that contains the email address of the system administrator, or a property that contains the number of expected vApp users.
- Some property values are entered by the user when the vApp is deployed, while other property values are configured by vCenter Server when the vApp is powered on. How properties are handled depends on the property type and the vCenter Server configuration.

When vCenter Server powers on a vApp, it creates an XML document that contains all properties and their values. This document is made available to each virtual machine in the vApp, and allows the virtual machines to apply the properties to their own environment.

Edit vApp Product Information for a Virtual Machine

If you want to export a virtual machine as an OVF template, you can specify product information that becomes available when you deploy a new virtual machine from the OVF template.

1. Navigate to a virtual machine from the vCenter Server inventory.
2. On the **Configure** tab, expand **Settings** and select **vApp options**.
3. Click the **Edit** button.
   The **Edit vApp Options** dialog box opens.
4. To enter product and vendor information, click the **Details** tab.

vApp Setting	Description
Name	Product name.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.
Vendor	Vendor name.
Vendor URL	If you enter a vendor URL, a user can click the vendor name from the **Summary** page of the virtual machine and go to the vendor's web page.

5. Click **OK**.

Manage vApp Custom Properties for a Virtual Machine

You can define and manage custom properties that are stored in the OVF template when you export a virtual machine or vApp and are used by vCenter Server when you deploy the OVF template. OVF templates support static properties, which are often configured by the user, and dynamic properties, which are always set by the vCenter Server.

To customize your virtual machine or vApp with properties, perform the following steps.

1. Define the OVF properties, for example a DNS address or gateway, in the virtual machine or vApp.
2. If you plan to export the virtual machine or the vApp to an OVF template:
   a. Set up the OVF environment transport to carry the settings into the virtual machine. See Edit OVF Details for a Virtual Machine .
   b. Write some glue-code to access and apply the information to the virtual machine.

See the VMware vApp Developer blog topic *Self-Configuration and the OVF Environment* for a discussion, sample code, and a video.

1. Navigate to a virtual machine from the vCenter Server inventory.
2. On the **Configure** tab, expand **Settings** and select **vApp options**.
3. You can manage custom properties from the **Properties** panel.

Option	Description
Add	To create a property, click **Add**.
Edit	To edit an existing property, select the property and click **Edit**.
Set Value	To set a new value to the existing property, select the property and click **Set Value**.
Delete	To delete an existing property, select the property and click **Delete**.

Edit vApp IP Allocation Policy for a Virtual Machine

You can set or edit the IP allocation policy that the virtual machine uses when you export it to an OVF template and deploy the OVF template.

1. Navigate to a virtual machine from the vCenter Server inventory.
2. On the **Configure** tab, expand **Settings** and select **vApp options**.
3. Click the **Edit** button.
   The **Edit vApp Options** dialog box opens.
4. If vApp options are not enabled, select the **Enable vApp options** check box.
5. Select the **IP protocol** and an **IP allocation scheme**.

   The supported protocols are IPv4, IPv6, or both.

   Consult the following table to learn more about the IP allocation schemes.

Option	Description
OVF environment	IP allocation is determined by the environment in which you deploy the OVF template.
DHCP	The IP addresses are allocated through a DHCP server when the virtual machine is powered on.

   The information you specify in the Authoring section will be used if you export the virtual machine to OVF and deploy the OVF at a later time.
6. Click **OK**.

Edit OVF Details for a Virtual Machine

A virtual machine's OVF settings allow you to customize the OVF environment, OVF transport, and boot behavior after OVF deployment. You can edit and configure settings that affect the OVF environment in the Virtual Machine Properties dialog box.

vApp options must be enabled in order to access these options.

1. Navigate to a virtual machine from the vCenter Server inventory.
2. On the **Configure** tab, expand **Settings** and select **vApp options**.
3. Click the **Edit** button.
   The **Edit vApp Options** dialog box opens.
4. If vApp options are not enabled, select the **Enable vApp options** check box.
5. To customize the OVF settings for the virtual machine, click the **OVF Details** tab.

Option	Description
OVF environment transport	• If you select **ISO image**, an ISO image that contains the OVF template information is mounted in the CD-ROM drive. • If you select **VMware Tools**, the VMware Tools `guestInfo.ovfEnv` variable is initialized with the OVF environment document.
Installation boot	If you click **Enable**, the virtual machine reboots after the OVF deployment completes. You can specify the delay time in seconds before the virtual machine starts the reboot operation.

6. Click **OK** to save your changes.

   In the **vApp Options are enabled** pane, you can view the **OVF Settings** panel with information about the OVF settings.

7. Optional: To view information about the OVF environment settings, power on the virtual machine and click the **View OVF Environment** button in the **vApp Options are enabled** pane.

   The information is displayed in XML format.

Monitoring Solutions with the vCenter Solutions Manager

A solution is an extension of vCenter Server that adds new functions to the vCenter Server instance. In the vSphere Client, you can view an inventory of the installed solutions with their detailed information. You can also monitor the health status of the solutions.

VMware products that integrate with vCenter Server are also considered solutions. For example, vSphere ESX Agent Manager is a VMware solution that lets you manage host agents that add new capabilities to ESX and ESXi hosts.

You can also install a solution to add functionality from third-party technologies to the standard functions of vCenter Server. Solutions are typically delivered as OVF packages. You can install and deploy solutions from the vSphere Client. You can integrate the solutions into the vCenter Solutions Manager, which provides a list of all installed solutions.

If a virtual machine or vApp runs a solution, a custom icon represents it in the inventory of the vSphere Client. Each solution registers a unique icon to show that the solution manages the virtual machine or vApp. The icons show the power states (powered on, paused, or powered off). Solutions display more than one type of icon if they manage more than one type of virtual machine or vApp.

When you power on or power off a virtual machine or vApp, you are notified that you are operating with an object that is managed by the vCenter Solutions Manager. When you attempt another operation on a virtual machine or a vApp that is managed by a solution, an informational warning message appears.

For more information, see the *Developing and Deploying vSphere Solutions, vServices, and ESX Agents* documentation.

View Solutions

vCenter Solutions Manager helps to deploy, monitor, and interact with solutions that are installed in a vCenter Server instance.

The vCenter Solutions Manager displays information about the solution, such as the solution name, the vendor name, and the version of the product. The vCenter Solutions manager also displays information about the health of a solution.

1. Navigate to the vCenter Solutions Manager.
   a) In the vSphere Client, select **Menu** > **Administration**.
   b) Expand **Solutions** and click **vCenter Server Extensions**.
2. Click a solution from the list.

   For instance, vService Manager or vSphere ESX Agent Manager.
3. Navigate through the tabs to view information about the solution.
   - **Summary**: You can view details about the solution, such as the product name, a short description, and links to the product and vendor websites. You can also view the solution configuration and the solution UI.

     Select the vCenter Server link to view the **Summary** page of the Virtual Machines or vApp.
   - **Monitor**: You can view the tasks and events related to the solution.
   - **VMs**: You can view a list of all the Virutal Machines and vApps that belong to the solution.

vSphere ESX Agent Manager

The vSphere ESX Agent Manager automates the process of deploying and managing ESX and ESXi agents, which extend the function of the host to provide additional services to a vSphere solution.

The vCenter Solutions Manager displays information about the vSphere ESX Agent Manager. The details include extension, related tasks and events, ESX agencies, agency related issues, and a list of the Virtual Machines and vApps that belong to the Agent Manager.

Monitor ESX Agent Health Status

The vCenter Solutions Manager displays the vSphere ESX Agent Manager that tracks the health status of agents on ESX/ESXi hosts.

vCenter Solutions Manager keeps track of whether the agents of a solution work as expected. Outstanding issues are reflected by the solution's ESX Agent Manager status and list of issues.

When there is a change in the current status of the solution's outstanding issues, the vCenter Solutions manager updates the ESX Agent Manager summary status and state. Administrators use this status to track whether the goal state is reached or not.

Table 167: ESX Agent Manager Health Status

Health Status Color	Description
Red	The solution must intervene for the ESX Agent Manager to proceed. For example, if a virtual machine agent is powered off manually on a compute resource and the ESX Agent Manager does not attempt to power on the agent. The ESX Agent Manager reports this action to the solution, and the solution alerts the administrator to power on the agent.
Yellow	The ESX Agent Manager is actively working to reach a goal state. The goal state can be enabled, disabled, or uninstalled. For example, when a solution is registered, its status is yellow until the ESX Agent Manager deploys the solutions agents to all the specified compute resources. A solution does not need to intervene when the ESX Agent Manager reports its ESX Agent Manager health status as yellow.
Green	A solution and all its agents have reached the goal state.

Resolve Agency Issues

ESX agencies provide an overview of all the issues related to ESX agents. You can resolve a single issue in the agency runtime information or you can resolve all issues at once.

ESX agencies are containers for ESX agents. ESX agencies aggregate information about the agents that they manage and all the issues that relate to those ESX agents.

1. Navigate to the vCenter Solutions Manager.
   a) In the vSphere Client, select **Menu** > **Administration**.
   b) Expand **Solutions** and click **vCenter Server Extensions**.
2. Select vSphere ESX Agent Manager and click the **Configure** tab.

   In the ESX Agencies pane, you can see a list of all agencies along with its cluster and solution information. You can click on a cluster name, to view the details of that cluster.

3. Select your task.
   - Resolve a single agency issue.
     a. Select an agency.
        Below the agency list, you can see a list of all the issues that are related to the selected agency.
     b. Select an issue from the list of issues for the selected agency.
     c. Click the vertical ellipsis icon and click **Resolve Issue**.
   - Resolve all agency issues.
     a. Select an agency.
     b. Click the vertical ellipsis icon and click **Resolve All Isues**.
        All the issues that are related to the selected agencies are resolved.

Managing Virtual Machines

You can manage individual virtual machines or a group of virtual machines that belongs to a host or cluster.

From the virtual machine's console, you can change the guest operating system settings, use applications, browse the file system, monitor system performance, and so on. Use snapshots to capture the state of the virtual machine at the time you take the snapshot.

To migrate virtual machines using cold or hot migration, including vMotion, vMotion in environments without shared storage, and Storage vMotion, see the *vCenter Server and Host Management* documentation.

Installing a Guest Operating System

A virtual machine is not complete until you install the guest operating system and VMware Tools. Installing a guest operating system in your virtual machine is essentially the same as installing it in a physical computer.

The basic steps for a typical operating system are described in this section. See the *Guest Operating System Installation Guide* at http://partnerweb.vmware.com/GOSIG/home.html.

Using PXE with Virtual Machines

You can start a virtual machine from a network device and remotely install a guest operating system using a Preboot Execution Environment (PXE). You do not need the operating system installation media. When you turn on the virtual machine, the virtual machine detects the PXE server.

PXE booting is supported for Guest Operating Systems that are listed in the VMware Guest Operating System Compatibility list and whose operating system vendor supports PXE booting of the operating system.

The virtual machine must meet the following requirements:

- Have a virtual disk without operating system software and with enough free disk space to store the intended system software.
- Have a network adapter connected to the network where the PXE server resides.

For details about guest operating system installation, see the *Guest Operating System Installation Guide* at http://partnerweb.vmware.com/GOSIG/home.html.

Install a Guest Operating System from Media

You can install a guest operating system from a CD-ROM or from an ISO image. Installing from an ISO image is typically faster and more convenient than a CD-ROM installation.

- Verify that the installation ISO image is present on a VMFS datastore or network file system (NFS) volume accessible to the ESXi host.
  Alternatively, verify that an ISO image is present in a content library.
- Verify that you have the installation instructions that the operating system vendor provides.

1. Log in to the vCenter Server system or host on which the virtual machine resides.
2. Select an installation method.

Option	Action
CD-ROM	Insert the installation CD-ROM for your guest operating system into the CD-ROM drive of your ESXi host.
ISO image	1. Right-click the virtual machine and select **Edit Settings**. The virtual machine Edit Settings dialog box opens. If the **Virtual Hardware** tab is not preselected, select it. 2. Select **Datastore ISO File** from the CD/DVD drop-down menu, and browse for the ISO image for your guest operating system.
ISO image from a Content Library	1. Right-click the virtual machine and select **Edit Settings**. The virtual machine Edit Settings dialog box opens. If the **Virtual Hardware** tab is not preselected, select it. 2. Select **Content Library ISO File** from the CD/DVD drop-down menu, and select an ISO image from the content library items.

3. Right-click the virtual machine and select **Power On**.
   A green right arrow appears next to the virtual machine icon in the inventory list.
4. Follow the installation instructions that the operating system vendor provides.

Install VMware Tools. VMware highly recommends running the latest version of VMware Tools on your guest operating systems. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience without them.

Upload ISO Image Installation Media for a Guest Operating System

You can upload an ISO image file to a datastore from your local computer. You can do this when a virtual machine, host, or cluster does not have access to a datastore or to a shared datastore that has the guest operating system installation media that you require.

Required privileges:
- **Datastore** > **Browse datastore** on the datastore.
- **Datastore** > **Low level file operations** on the datastore.
- **Host** > **Configuration** > **System Management**

1. In the vSphere Client, select **Menu** > **Storage**.
2. Select the datastore from the inventory to which you will upload the file.
3. Optional: On the **Files** tab, click the **New Folder** icon to create a new folder.
4. Select an existing folder or the folder that you created, and click the **Upload Files** icon.
5. On the local computer, find the file and upload it.
   ISO upload times vary, depending on file size and network upload speed.
6. Refresh the datastore file browser to see the uploaded file in the list.

After you upload the ISO image installation media, you can configure the virtual machine CD-ROM drive to access the file.

Customizing Guest Operating Systems

When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine. You can change the computer name, network settings, and license settings.

Customizing guest operating systems helps prevent conflicts that occur if virtual machines with identical settings are deployed, for example conflicts due to duplicate computer names. You can apply customization as part of virtual machine deployment or later.

- During the cloning or deployment process, you can specify customization settings or you can select an existing customization specification.
- You can create a customization specification explicitly from the **Policies and Profiles** and apply it to a virtual machine.

Guest Operating System Customization Requirements

To customize the guest operating system, you must configure the virtual machine and guest to meet VMware Tools and virtual disk requirements. Other requirements apply, depending on the guest operating system type.

VMware Tools Requirements

The latest version of VMware Tools must be installed on the virtual machine or template to customize the guest operating system during cloning or deployment. For information about VMware Tools support matrix, see the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Virtual Disk Requirements

The guest operating system being customized must be installed on a disk attached as SCSI node 0:0 in the virtual machine configuration.

Windows Requirements

Customization of Windows guest operating systems requires the virtual machine to be running on an ESXi host running version 3.5 or later.

Linux Requirements

Customization of Linux guest operating systems requires that Perl is installed in the Linux guest operating system.

Verifying Customization Support for a Guest Operating System

To verify customization support for Windows operating systems or Linux distributions and compatible ESXi hosts, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility. You can use this online tool to search for the guest operating system and ESXi version. After the tool generates your list, click the guest operating system to see whether guest customization is supported.

Create a vCenter Server Application to Generate Computer Names and IP Addresses

Instead of entering computer names and IP addresses for virtual NICs when you customize guest operating systems, you can create a custom application and configure it in such a way that vCenter Server generates the names and addresses.

Verify that Perl is installed on vCenter Server.

The application can be an arbitrary executable binary or script file appropriate for the corresponding operating system in which vCenter Server is running. After you configure an application and make it available to vCenter Server, every time you initiate a guest operating system customization for a virtual machine, vCenter Server runs the application.

The application must comply with the reference XML file in the VMware knowledge base article at http://kb.vmware.com/kb/2007557.

1. Create the application and save it on the vCenter Server system's local disk.
2. Select a vCenter Server instance in the inventory.
3. Click the **Configure** tab, click **Settings**, and click **Advanced Settings**.
4. Click **Edit Settings** and enter the configuration parameters for the script.
   a) In the **Name** text box, enter `config.guestcust.name-ip-generator.arg1`.
   b) In the **Value** text box, enter `c:\sample-generate-name-ip.pl` and click **Add**.
   c) In the **Name** text box, enter `config.guestcust.name-ip-generator.arg2`.
   d) In the **Value** text box, enter the path to the script file on the vCenter Server system and click **Add**. For example, enter `c:\sample-generate-name-ip.pl`.
   e) In the **Name** text box, enter `config.guestcust.name-ip-generator.program`.
   f) In the **Value** text box, enter `c:\perl\bin\perl.exe` and click **Add**.
5. Click **Save**.

You can select the option to use an application to generate computer names or IP addresses during guest operating system customization.

Customize Windows During Cloning or Deployment

You can customize the Windows guest operating systems of the virtual machines when you deploy a new virtual machine from a template or clone an existing virtual machine. Customizing the guest operating system helps prevent conflicts that might result if you or other users deploy virtual machines with identical settings, such as duplicate computer names.

- Verify that all requirements for customization are met. See Guest Operating System Customization Requirements.
- Verify that there are customization specifications available for use. For information about creating a guest customization specification, see Create a Customization Specification for Windows.

You can prevent Windows from assigning new virtual machines or templates with the same Security IDs (SIDs) as the original virtual machine. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

Important: After customization, the default administrator password is not preserved for Windows Server 2008. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine starts the first time after customization.

1. Right-click any inventory object that is a valid parent object of a virtual machine, such as data center, cluster, vApp, resource pool, or host, and select **New Virtual Machine**.
2. On the **Select a creation page**, select **Clone an existing virtual machine** or **Deploy from template**.
3. Click **Next**.
4. Follow the prompts until you reach the **Select clone options** page.
5. On the **Select clone options** page, select the **Customize the operating system** check box and click **Next.**
6. On the **Customize guest OS** page, apply a customization specification to the virtual machine, and click **Next**.

Option	Action
Select an existing specification	Select a customization specification from the list.

Option	Action
Override	To change the guest customization specification for this deployment only, click **Override**, complete the steps in the **Override VM Customization Specification** wizard, and click **OK**.

7. On the **User settings** page, specify the required settings for the virtual machine.
   This page of the wizard appears only if the selected specification requires additional customization.
8. On the **Ready to complete** page, review the details and click **Finish**.

When the new virtual machine starts for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might restart several times during this process.

If the guest operating system pauses when the new virtual machine starts, it might be waiting for you to correct errors, such as an incorrect product key or an invalid user name. To determine whether the system is waiting for information, open the virtual machine console.

After you deploy certain Windows operating systems that are not volume licensed, you might need to reactivate your operating system on the new virtual machine.

If the new virtual machine encounters customization errors while it is starting, the errors are logged to `%WINDIR%\temp\vmware-imc`. To view the error log file, from the Windows **Start** menu navigate to **Programs** > **Administrative Tools** > **Event Viewer**.

Customize Linux During Cloning or Deployment

In the process of deploying a new virtual machine from a template or cloning an existing virtual machine, you can customize the Linux guest operating systems of the virtual machines.

- Verify that all requirements for customization are met. See Guest Operating System Customization Requirements.
- Verify that there are customization specifications available for use. For information about creating a guest customization specification, see Create a Customization Specification for Linux.

1. Right-click any inventory object that is a valid parent object of a virtual machine, such as data center, cluster, vApp, resource pool, or host, and select **New Virtual Machine**.
2. On the **Select a creation page**, select **Clone an existing virtual machine** or **Deploy from template**.
3. Click **Next**.
4. Follow the prompts until you reach the **Select clone options** page.
5. On the **Select clone options** page, select the **Customize the operating system** check box and click **Next.**
6. On the **Customize guest OS** page, apply a customization specification to the virtual machine, and click **Next**.

Option	Action
Select an existing specification	Select a customization specification from the list.
Override	To change the guest customization specification for this deployment only, click **Override**, complete the steps in the **Override VM Customization Specification** wizard, and click **OK**.

7. On the **User settings** page, specify the required settings for the virtual machine.
   This page of the wizard appears only if the selected specification requires additional customization.

8. On the **Ready to complete** page, review the details and click **Finish**.

When the new virtual machine starts for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might restart several times during this process.

If the guest operating system pauses when the new virtual machine starts, it might be waiting for you to correct errors, such as an incorrect product key or an invalid user name. To determine whether the system is waiting for information, open the virtual machine console.

If the new virtual machine encounters customization errors while it is starting, the errors are reported using the guest's system logging mechanism. View the errors in the `/var/log/vmware-imc/toolsDeployPkg.log` file.

Apply a Customization Specification to an Existing Virtual Machine

You can apply a customization spec to an existing virtual machine. Using customization specs helps prevent conflicts that can result if you deploy virtual machines with identical settings, such as duplicate computer names.

- Verify the guest operating system is installed.
- Verify that VMware Tools is installed and running.
- Power off the virtual machine.

When you clone an existing virtual machine, or deploy a virtual machine from a VM template in a folder, you can customize the guest operating system of the resulting virtual machine during the clone or the deployment tasks.

When you deploy a virtual machine from a template in a content library, you can customize the guest operating system only after the deployment task is complete.

1. Right-click a virtual machine in the vSphere inventory, and select **Guest OS** > **Customize Guest OS**.

   The **Customize Guest OS** dialog box opens.

2. Select a customization specification from the list and click **OK**.

   If the specification requires you to configure additional settings, a new dialog box opens and your are prompted to enter information about the required settings.

Creating and Managing Customization Specifications

You can create and manage customization specifications for Windows and Linux guest operating systems. Customization specifications are XML files that contain guest operating system settings for virtual machines. When you apply a specification to the guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

vCenter Server saves the customized configuration parameters in the vCenter Server database. If the customization settings are saved, the administrator and domain administrator passwords are stored in encrypted format in the database. Because the certificate used to encrypt the passwords is unique to each vCenter Server system, if you reinstall vCenter Server or attach a new instance of the server to the database, the encrypted passwords become invalid. You must reenter the passwords before you can use them.

To learn how you can create and manage customization specifications in the , watch the following video.

Create a Customization Specification for Linux

Save the system settings for a Linux guest operating system in a customization specification, which you can apply when cloning virtual machines or deploying virtual machines from templates.

- Verify that all requirements for customization are met. See Guest Operating System Customization Requirements.

- To run the customization script:
  - Verify that VMware Tools version 10.1.0 or later is installed. The customization fails if VMware Tools is version earlier than 10.1.0 and you attempt to run the customization script.
  - In the VMware Tools configuration, the `enable-custom-scripts` option is deactivated by default for security reasons. When you attempt to run the customization script with a deactivated `enable-custom-scripts` option, the customization fails with a customization error.

    For example, to enable the `enable-custom-scripts` option, you must run `vmware-toolbox-cmd` as root user with the `config` command:

    ```
    vmware-toolbox-cmd config set deployPkg enable-custom-scripts true
    cat /etc/vmware-tools/tools.conf
    [deployPkg]
    enable-custom-scripts = true
    ```

    To verify that you set the option correctly, you can run the following command:

    ```
    vmware-toolbox-cmd config get deployPkg enable-custom-scripts
    [deployPkg] enable-custom-scripts = true
    ```

    For more information, see the *VMware Tools User Guide*.

1. Select **Menu** > **Policies and Profiles**, and under Policies and Profiles, click **VM Customization Specifications**.
2. Click the **Create a new specification** icon.

   The **New VM Guest Customization Specification** wizard starts.
3. On the **Name and target OS** page, enter a name and a description for the customization specification, select **Linux** as a target guest OS, and click **Next**.
4. On the **Computer name** page, enter a computer name for the guest operating system and a domain name.

   The operating system uses the computer name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Use the virtual machine name	Select this option to use the virtual machine name. The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	Select this option to be prompted to enter a name during cloning or deployment.
Enter a name	1. Enter a name. The name can contain alphanumeric characters and a hyphen (-). It cannot contain a period (.), blank spaces, or special characters, and cannot contain digits only. Names are not case-sensitive. 2. To ensure that the name is unique, select the **Append a numeric value** check box. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.
Generate a name using the custom application configured with vCenter Server	Optional: Enter a parameter that can be passed to the custom application.

5. Enter the **Domain Name** for the computer and click **Next**.
6. On the **Time zone** page, select the time zone for the virtual machine and click **Next**.
7. On the **Customization script** page, apply a customization script to the guest operating system of the VM and click **Next**.
   a) To upload a file containing the customization script, click **Browse** and navigate to the file on your local machine. The contents of the script appear in the **Script** text box.
   b) (Optional) Enter the customization script directly into the **Script** text box.

   The customization script cannot exceed 1500 characters.

   Note:

   The default timeout period for the guest customization to complete is set to 100 seconds and includes the time for the script to run when you use a `"precustomization"` command-line parameter. If you run scripts that take a time exceeding the timeout, the guest customization fails.

   When you add a customization script with the `"precustomization"` command-line parameter, it is called before the guest customization begins. As a result, the virtual NIC is disconnected and you cannot access the network.

   When you add a customization script with the `"postcustomization"` command-line parameter, it is called after the guest customization finishes. As a result, the script is scheduled in the initialization process after the virtual machine powers on, the NIC is connected, and you can access the network. The time for the script to run is not included in the default timeout period and you avoid a guest customization failure.

   Customization Script Example

   ```
   #!/bin/sh
   if [ x$1 == x"precustomization" ]; then
   echo Do Precustomization tasks
   elif [ x$1 == x"postcustomization" ]; then
   echo Do Postcustomization tasks
   fi
   ```

8. On the **Network** page, select the type of network settings to apply to the guest operating system and click **Next**.
   - Select **Use standard network settings** so that vCenter Server configures all network interfaces from a DHCP server by using the default settings.
   - Select **Manually select custom settings** and manually configure each network interface.
     a. Select a network adapter from the list or add a new one.
     b. For the selected NIC, click **Edit**.
        The **Edit Network** dialog box opens.
     c. To configure the virtual machine to use an IPv4 network, click the **IPv4** tab.
        If you select the **Prompt the user for an IPv4 address when the specification is used** option, vCenter Server prompts for an IP address when you select to apply the customization specification during cloning or deployment. You are also prompted to configure the gateways during cloning and deployment.
     d. To configure the virtual machine to use an IPv6 network, click the **IPv6** tab.
        If you select the **Prompt the user for an address when the specification is used** option, vCenter Server prompts for an IP address when you select to apply the customization specification during cloning or deployment. You are also prompted to configure the gateways during cloning and deployment.
     e. Click **OK**.
9. On the **DNS settings** page, enter DNS server and domain settings.

   The **Primary DNS**, **Secondary DNS**, and **Tertiary DNS** text boxes accept both IPv4 and IPv6 addresses.

10. On the **Ready to complete** page, review the details and click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Create a Customization Specification for Windows

Save specific Windows guest operating system settings in a customization specification, which you can apply when cloning virtual machines or deploying from templates.

Ensure that all requirements for customization are met. See Guest Operating System Customization Requirements.

Note: The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine starts the first time after customization.

1. Select **Menu** > **Policies and Profiles**, and under Policies and Profiles, click **VM Customization Specifications**.
2. Click the **Create a new specification** icon.

   The **New VM Guest Customization Specification** wizard opens.
3. On the **Name and target OS** page, enter a name and description for the customization specification and select **Windows** as a target guest OS.
4. Optional: Select the **Generate a new security identity (SID)** option and click **Next**.

   A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

   Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.
5. On the **Set Registration Information** page, enter the virtual machine owner's name and organization and click **Next**.
6. On the **Computer name** page, enter a computer name for the guest operating system and a domain name.

   The operating system uses the computer name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Use the virtual machine name	Select this option to use the virtual machine name. The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	Select this option to be prompted to enter a name during cloning or deployment.
Enter a name	1. Enter a name. The name can contain alphanumeric characters and a hyphen (-). It cannot contain a period (.), blank spaces, or special characters, and cannot contain digits only. Names are not case-sensitive. 2. To ensure that the name is unique, select the **Append a numeric value** check box. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.

Option	Action
Generate a name using the custom application configured with vCenter Server	Optional: Enter a parameter that can be passed to the custom application.

7. On the **Windows license** page, provide licensing information for the Windows operating system and click **Next**.

Option	Action
For nonserver operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	1. Type the Windows product key for the new guest operating system. 2. Select **Include Server License Information**. 3. Select either **Per seat** or **Per server**. 4. If you select **Per server**, enter the maximum number of simultaneous connections for the server to accept.

8. On the **Set Administrator Password** page, configure the administrator password for the virtual machine and click **Next**.
   a) Enter a password for the administrator account and confirm the password by typing it again.
   b) Optional: Select the **Automatically logon as Administrator** check box to log users in to the guest operating system as Administrator, and select the number of times to log in automatically.
9. On the **Time zone** page, select the time zone for the virtual machine and click **Next**.
10. Optional: On the **Run Once** page, specify commands to run the first time a user logs in to the guest operating system and click **Next**.

    See the Microsoft Sysprep documentation for information about `RunOnce` commands.
11. On the Network page, select the type of network settings to apply to the guest operating system and click **Next**.
    - Select **Use standard network settings** so that vCenter Server configures all network interfaces from a DHCP server by using the default settings.
    - Select **Manually select custom settings** and configure each network interface yourself.
      a. Select a network adapter from the list or add a new one.
      b. For the selected NIC, click the vertical ellipsis icon and select **Edit**.
         The **Edit Network** dialog box opens.
      c. Click the **IPv4** tab to configure the virtual machine to use IPv4 network.
         You can configure all the settings at that stage or you can select the **Prompt the user for an IPv4 address when the specification is used** option. In that case, vCenter Server prompts for an IP address when you select to apply that customization specification during cloning or deployment. With that option, you can also configure the gateways during cloning or deployment.
      d. Click the **IPv6** tab to configure the virtual machine to use IPv6 network.
         You can configure all the settings at that stage or you can select the **Prompt the user for an address when the specification is used** option. In that case, vCenter Server prompts for an IP address when you select to apply that customization specification during cloning or deployment. With that option, you can also configure the gateways during cloning or deployment.
      e. Click the **DNS** tab to specify DNS server details.
      f. Click **WINS** to specify primary and secondary WINS server information.
      g. Click **OK** to close the **Edit Network** dialog box.

12. On the **Set Workgroup or Domain** page, select how the virtual machine participates in the network and click **Next**.

Option	Action
Workgroup	Enter a workgroup name. For example, `MSHOME`.
Windows Server Domain	1. Enter the domain name. 2. To add a computer to the specified domain, enter the user name and password for a user account that has permission.

13. On the Ready to complete page, review the details and click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Create a Customization Specification for Windows Using a Custom Sysprep Answer File

A custom sysprep answer file is a file that stores various customization settings such as computer name, licensing information, and workgroup or domain settings. You can supply a custom sysprep answer file as an alternative to specifying many of the settings in the Guest Customization wizard.

Ensure that all requirements for customization are met. See Guest Operating System Customization Requirements.

Windows Server 2003 and Windows XP use a text file called `sysprep.inf`. Windows Server 2008, Windows Vista, and Windows 7 use an XML file called `sysprep.xml`. You can create these files using a text editor, or use the Microsoft Setup Manager utility to generate them. For more information about how to create a custom sysprep answer file, see the documentation for the relevant operating system.

Important: If you use a custom sysprep answer file to deploy a virtual machine with an operating system Windows Vista or later, you must specify the network customization specifications in the sysprep file. The custom network settings that you configure in the **New VM Guest Customization Specification** wizard are not applied. For more information, see VMware KB article 1029174 at https://kb.vmware.com/s/article/1029174.

You can prevent Windows from assigning new virtual machines or templates with the same Security IDs (SIDs) as the original virtual machine. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

1. Select **Menu** > **Policies and Profiles**, and under Policies and Profiles, click **VM Customization Specifications**.
2. Click the **Create a new specification** icon.

   The **New VM Guest Customization Specification** wizard opens.
3. On the Name and target OS page, enter a name and description for the customization specification and select **Windows** as a target guest OS.
4. Optional: Select the **Generate a new security identity (SID)** option.

   A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

   Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

5. Select **Use Custom Sysprep Answer File** and click **Next**.
6. On the Custom sysprep file, select the option to import or create a sysprep answer file and click **Next**.

Option	Description
Import a Sysprep answer file	Click **Browse** and browse to the file.
Create a Sysprep answer file	Type the contents of the file in the text box.

7. On the Network page, select the type of network settings to apply to the guest operating system and click **Next**.
   - Select **Use standard network settings** so that vCenter Server configures all network interfaces from a DHCP server by using the default settings.
   - Select **Manually select custom settings** and configure each network interface yourself.
     a. Select a network adapter from the list or add a new one.
     b. For the selected NIC, click the vertical ellipsis icon and select **Edit**.
        The **Edit Network** dialog box opens.
     c. Click the **IPv4** tab to configure the virtual machine to use IPv4 network.
        You can configure all the settings at that stage or you can select the **Prompt the user for an IPv4 address when the specification is used** option. In that case, vCenter Server prompts for an IP address when you select to apply that customization specification during cloning or deployment. With that option, you can also configure the gateways during cloning or deployment.
     d. Click the **IPv6** tab to configure the virtual machine to use IPv6 network.
        You can configure all the settings at that stage or you can select the **Prompt the user for an address when the specification is used** option. In that case, vCenter Server prompts for an IP address when you select to apply that customization specification during cloning or deployment. With that option, you can also configure the gateways during cloning or deployment.
     e. Click the **DNS** tab to specify DNS server details.
     f. Click **WINS** to specify primary and secondary WINS server information.
     g. Click **OK** to close the **Edit Network** dialog box.
8. On the Ready to complete page, review the details and click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Manage Customization Specifications

You can edit, duplicate, export, or delete existing specifications.

1. In the vSphere Client, select **Menu** > **Policies and Profiles** and click **VM Customization Specifications**.
2. Select a customization specification and select your task.

Option	Description
Edit customization spec	You can make changes to the customization spec, such as changing the networking configuration. Click **Edit** and make the necessary changes.
Duplicate customization spec	If you need a customization specification that is only slightly different from an existing specification, you can use the Customization Specification Manager to create a copy of the existing specification and modify it. For example, you might need to change the IP address or the administrator password.
Export customization spec	You can export customization specifications and save them as `.xml` files. To apply an exported specification to a virtual machine, import the .xml file using the **Import** button.
Delete specification spec	You can remove customization specifications to free up storage.

Import a Customization Specification

You can import an existing specification and use the specification to customize the guest operating system of a virtual machine.

Before you begin, you must have at least one customization specification saved as an xml file located on a file system accessible from the vSphere Client.

1. In the vSphere Client, select **Menu** > **Policies and Profiles** and click **VM Customization Specifications**.
2. Click the **Import** icon.
3. Browse to the `.xml` file to import, specify a name and optional description, and click **OK**.

The imported specification is added to the list of customization specifications.

Managing Power States of a Virtual Machine

The basic power operations for a virtual machine include powering on, powering off, suspending, reset, and hard stop. These power options are analogous to the power operations on a physical computer.

Verify that you have the following privileges:

- **VirtualMachine** > **Interaction** > **PowerOn**
- **VirtualMachine** > **Interaction** > **PowerOff**
- **VirtualMachine** > **Interaction** > **Suspend**
- **VirtualMachine** > **Interaction** > **Reset**

For information about how to change the virtual machine power states, see Configure the Virtual Machine Power States.

1. Navigate to a virtual machine in the inventory.
2. Right-click the virtual machine or click **Actions**, and select **Power**.
3. Select a power operation.

Option	Description
Power On	Powers on a virtual machine when the virtual machine is stopped.
Power Off	Powers off a virtual machine. Powering off a virtual machine might cause loss of data within the guest operating system.
Suspend	Suspends a running virtual machine and leaves it connected to the network. When you resume a suspended virtual machine, the virtual machine continues operating at the same point the virtual machine was at when it was suspended.
Reset	Restarts the guest operating system. By using this operation, the virtual machine powers off and then powers on. By resetting a virtual machine, you might lose all unsaved information within the guest operating system.
Hard stop	You can use this operation only when you cannot power off a virtual machine or if a virtual machine becomes unresponsive. When you hard stop a virtual machine, all processes are ended and the virtual machine is powered off. By using this operation, you might lose all unsaved information.

Edit Virtual Machine Startup and Shutdown Settings

You can configure virtual machines running on an ESXi host to start up and shut down with the host or after a delay. You can also set the default timing and startup order for virtual machines. This way, the operating system has enough time to save data when the host enters maintenance mode or is being powered off for another reason.

The Virtual Machine Startup and Shutdown (automatic startup) setting is deactivated for all virtual machines residing on hosts that are in a vSphere HA cluster. Automatic startup is not supported with vSphere HA.

Note: You can also create a scheduled task to change the power settings for a virtual machine. See *vCenter Server and Host Management*.

1. In the vSphere Client, navigate to and select the host where the virtual machine is located.
2. Click the **Configure** tab.
3. Under **Virtual Machines**, select **VM Startup/Shutdown** and click **Edit**.
   The **Edit VM Startup/Shutdown Configuration** dialog box opens.
4. Select **Automatically start and stop the virtual machines with the system**.
5. Optional: In the **Default VM Settings** pane, configure the default startup and shutdown behavior for all virtual machines on the host.

Setting	Description
Startup Delay	After you start the ESXi host, it starts powering on the virtual machines that are configured for automatic startup. After the ESXi host powers on the first virtual machine, the host waits for the specified delay time and then powers on the next virtual machine. The virtual machines are powered on in the startup order specified under the **Default VM Settings** pane.
Continue if VMware Tools is started	Shortens the startup delay of the virtual machine. If VMware Tools starts before the specified delay time passes, the ESXi host powers on the next virtual machine without waiting for the delay time to pass.
Shutdown delay	Shutdown delay is the maximum time the ESXi host waits for a shutdown command to complete. When you power off the ESXi host, the autostart manager initiates the automatic shutdown on the first virtual machine and waits within the specific delay time for the virtual machine to complete the power action. The power action can be Power Off, Guest Shutdown, or Suspended. The order in which virtual machines are shut down is the reverse of their startup order. After the ESXi host shuts down the first virtual machine within the time that you specify, the host shuts down the next virtual machine. If a virtual machine does not shut down within the specified delay time, the host runs a power off command and then starts shutting down the next virtual machine. The ESXi host shuts down only after all virtual machines are shut down.
Shutdown action	Select a shutdown action that is applicable to the virtual machines on the host when the host shuts down. • **Guest Shutdown** • **Power Off** • **Suspend** • **None**

6. Optional: You can also configure the startup order and behavior for individual virtual machines.

   Use this option when you need the delay of the virtual machine to be different from the default delay for all machines. The settings that you configure for individual virtual machines override their default settings.

   a) To change the startup order of virtual machines, select a virtual machine from the **Manual Startup** category and use the up arrow to move it up to the **Automatic** or **Automatic Ordered** categories.

      Use the up and down arrows to change the startup order for virtual machines in the **Automatic** and **Manual Startup** categories. During shutdown, the virtual machines shut down in the reverse order.

   b) To edit the startup and shutdown behavior of a virtual machine, select a virtual machine, use the up arrow to move it, and click the **Edit** icon.

      The **Virtual Machine Startup/Shutdown setting** dialog box opens.

   c) In the **Startup Settings** pane, configure the startup behavior of the virtual machine.

      You can decide to use the default startup delay or you can specify a new one. If you select **Continue immediately if VMware Tools starts**, the ESXi host powers on the next virtual machine without waiting for the delay to pass.

   d) In the **Shutdown Settings** pane, configure the shutdown behavior of the virtual machine.

      You can use the default shutdown delay or specify a new one and select the shutdown action.

   e) Click **OK**.

7. Click **OK**.

Using a Virtual Machine Console

With the vSphere Client, you can access a virtual machine's console by displaying it in a separate Web browser, or from the VMware Remote Console (VMRC).

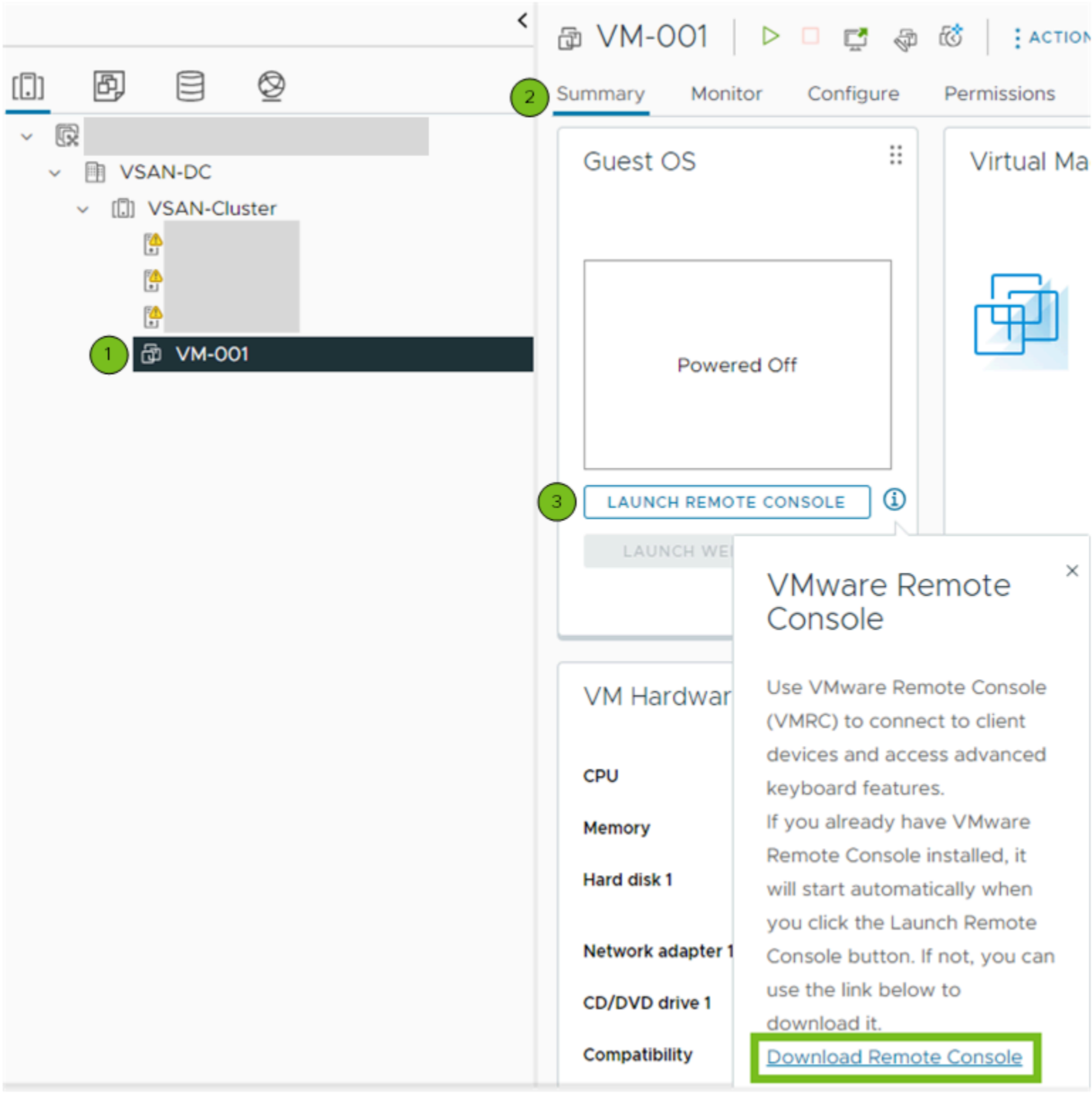
From the virtual machine remote console, you can perform tasks in the virtual machine such as installing an operating system, configuring the operating system settings, running applications, monitoring performance, and so on. The vSphere Client offers these choices:

- Launch the Web console to display the VM console in a separate browser tab.
- Download the VMware Remote Console (VMRC) standalone application, which opens in a separate window. The VMware Remote Console standalone application enables you to connect to client devices and launch virtual machine consoles on remote hosts.

Install the VMware Remote Console Application

The VMware Remote Console (VMRC) is a standalone console application. VMRC enables you to connect to client devices and open virtual machine consoles on remote hosts.

Download the VMRC if you do not already have the VMRC installed.

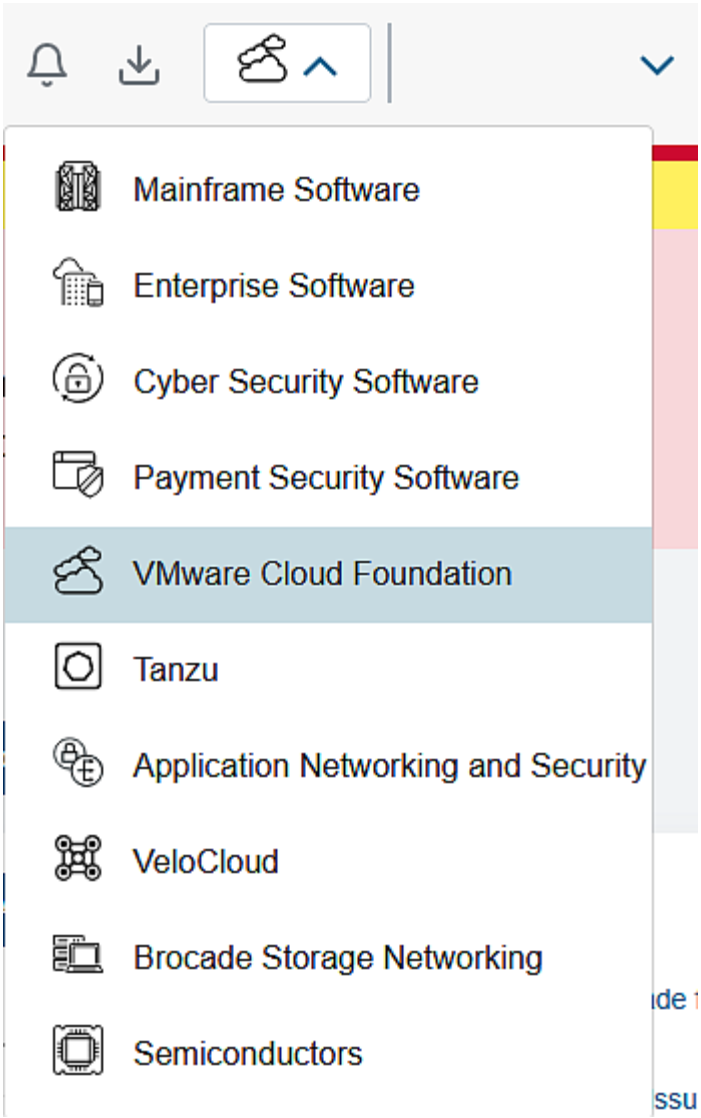

VM-001
ACTION
2
Summary
Monitor
Configure
Permissions
VSAN-DC
VSAN-Cluster
1
VM-001
Guest OS
Virtual Ma
Powered Off
3
LAUNCH REMOTE CONSOLE
VM Hardwar
CPU
Memory
Hard disk 1
Network adapter 1
CD/DVD drive 1
Compatibility
VMware Remote Console
Use VMware Remote Console (VMRC) to connect to client devices and access advanced keyboard features.
If you already have VMware Remote Console installed, it will start automatically when you click the Launch Remote Console button. If not, you can use the link below to download it.
Download Remote Console

1. In the vSphere Client, navigate to a virtual machine in the inventory.
2. Click the **Summary** tab.
3. From the **Launch Remote Console** link, click the information icon ( ) and click **Download Remote Console**.
4. Download the VMRC installer from the Broadcom website at https://support.broadcom.com.

   Note:

   You must have a profile at https://support.broadcom.com to download the VMRC installer.

   a) Log in to the Broadcom Support Portal with your credentials.
   b) From the drop-down menu, select **VMware Cloud Foundation**.



c) From the side navigation menu, click **My Downloads** and enter `VMware vSphere` in the **Search Product Name** bar.
d) Click **Show Results** and click **VMware vSphere**.
e) Click the **Products** tab and expand **VMware vSphere - Enterprise** from the list.
f) Click the release version and click the **Drivers & Tools** tab.
g) In the **Search** bar, enter `VMware Remote Console`.
The list with VMRC versions appears.
h) Expand the version you want to download and click the download ( ) icon.

Start the VMware Remote Console Application

You can use the standalone VMRC application to connect to client devices.

- Verify that VMRC is installed on your local system. You can download the VMRC installer from the VMware website at https://customerconnect.vmware.com/en/downloads.
- Verify that you have the **Virtual machine** > **Interaction** > **Console interaction** privilege.

With VMRC, you can access the mouse and keyboard connected to remote virtual machines. To perform administrative tasks, you must log in to the VMRC as an administrator.

1. In the vSphere Client, navigate to a virtual machine in the inventory.
2. On the **Summary** tab, click **Launch Remote Console**.
   A dialog box opens that requires you to confirm that you want to open the remote console.
3. In the **Open VMware Remote Console** dialog box, confirm that you want to open VMRC.
   The VMRC opens as a standalone application for the selected virtual machine. You can also run more than one console to access remotely several virtual machines at the same time.

Open the Web Console

You can access a virtual machine desktop from the vSphere Client by opening the web console and performing various tasks in the virtual machine. For example, you can install an operating system, configure the operating system settings, run applications, monitor performance, and so on.

- Verify that the virtual machine has a guest operating system and that VMware Tools is installed.
- Verify that the virtual machine is powered on.
- Verify that you have the **Virtual machine** > **Interaction** > **Console interaction** privilege.

1. In the vSphere Client, navigate to a virtual machine in the inventory.
2. In the **Summary** tab, select **Launch Web Console**.
   The console opens in a new browser tab.
3. Click anywhere inside the console window to start using your mouse, keyboard, and other input devices in the console.

   Note: For information about supported international keyboards, refer to the VMware HTML Console SDK Release Notes at https://www.vmware.com/support/developer/html-console/html-console-21-releasenotes.html#knownissues.

4. Optional: Click **Send Ctrl-Alt-Delete** to send the Ctrl+Alt+Delete keystroke combination to the guest operating system.
5. Optional: Press Ctrl+Alt to release the pointer from the console window and work outside the console window.
6. Optional: Click **Full Screen** to view the console in full screen mode.
7. Optional: Press Ctrl+Alt+Enter to enter or exit full screen mode.

Manage the VMware Remote Console Proxy Configuration

VMware Remote Console proxy for vSphere (VMRC proxy) is a service in the vCenter Server system which transmits the network traffic between VMRC and the ESXi hosts. When you use the VMRC proxy, VMRC does not require a direct network connection to the ESXi host.

You can activate or deactivate the VMRC proxy. You also can change the VMRC proxy settings to reduce the workload on the vCenter Server system.

Activate the VMware Remote Console Proxy

The VMRC proxy is deactivated by default. You can activate the VMRC proxy service through **Advanced Settings** of your vCenter Server system.

Verify that you have the **Global.Settings** privilege.

1. In the vSphere Client, navigate to and select the vCenter Server instance.
2. On the **Configure** tab, select **Advanced Settings**.
3. Click **Edit Settings**.
   The **Edit Advanced vCenter Server Settings** dialog box opens.
4. In the **Name** text box, enter the name of the service - `config.mksdevproxy.enable`.
5. In the **Value** text box, enter `true` and click **Add**.
6. Click **Save**.
   The proxy setting appears in the list containing all configuration parameters.

Deactivate the VMware Remote Console Proxy

To simplify your vCenter Server configuration, you can deactivate the VMRC proxy.

Verify that you have the **Global.Settings** privilege.

1. In the vSphere Client, navigate to and select the vCenter Server instance.
2. On the **Configure** tab, select **Advanced Settings**.
3. Click **Edit Settings**.
   The **Edit Advanced vCenter Server Settings** dialog box opens.

4. Click the **Filter** icon in the **Name** column.
5. To view the VMRC proxy parameter, in the text box, enter `config.mksdevproxy.enable` and close the dialog box.
6. In the **Value** text box, enter `false`, and click **Save**.

Manage the VMware Remote Console Proxy Settings

To ensure that the vCenter Server system performs efficiently, you can change the settings of VMRC proxy. You can configure the number of concurrent VMRC proxy connections and the maximum bandwith for each concurrent VMRC proxy connection.

Configure a Concurrent VMRC Proxy Connection
The VMRC network traffic might impact the work of the vCenter Server instance and you can limit the number of the concurrent VMRC proxy connections.

Verify that you have the **Global.Settings** privilege.

To ensure that the vCenter Server performance is optimum, configure the number of the concurrent VMRC proxy connections to be between 1 and 1024. To meet your configuration needs, you can change the maximum concurrent VMRC proxy connections. By default, the maximum number of concurrent VMRC proxy connections is 32.

1. In the vSphere Client, navigate to and select the vCenter Server instance.
2. On the **Configure** tab, select **Advanced Settings**.
3. Click **Edit Settings**.
4. Configure the number of the concurrent VMRC proxy connections.

Option	Action
Configure a concurrent VMRC proxy connection	1. In the **Name** text box, enter `config.mksdevproxy.connLimit`. 2. In the **Value** text box, enter a value for the maximum number of concurrent connections allowed. 3. Click **Add**.
Limit the number of the VMRC proxy connections	1. Click the **Filter** icon in the **Name** column. 2. To view the VMRC proxy parameter, in the text box enter `config.mksdevproxy.connLimit` and close the dialog box. 3. In the **Value** text box, change the number of the concurrent connections.

5. Click **Save**.

Configure the Maximum Bandwidth for a Concurrent VMRC Proxy Connection
You can limit the number of the available network bandwidth.

Verify that you have the **Global.Settings** privilege.

Each concurrent connection has a maximum of 300 KBps network bandwidth. VMRC requires minimum 50 KBps for the basic mouse, keyboard, and screen transfer.

1. In the vSphere Client, navigate to and select the vCenter Server instance.
2. On the **Configure** tab, select **Advanced Settings**.
3. Click **Edit Settings**.
4. Configure the maximum bandwidth for each concurrent VMRC proxy connection.

Option	Action
Configure the VMRC inbound traffic to the vCenter Server system	1. In the **Name** text box, enter `config.mksdevproxy.readthrottler`. 2. In the **Value** text box, enter the value of the inbound traffic in KBps. 3. Click **Add**.
Configure the vCenter Server outbound traffic to VMRC	1. In the **Name** text box, enter `config.mksdevproxy.writethrottler`. 2. In the **Value** text box, enter the value of the outbound traffic in KBps. 3. Click **Add**.
Limit the VMRC inbound traffic to the vCenter Server system	1. Click the **Filter** icon in the **Name** column. 2. To display the VMRC proxy parameter, in the text box, enter `config.mksdevproxy.readthrottler` and close the dialog box. 3. In the **Value** text box, enter the inbound bandwidth limit in KBps.
Limit the vCenter Server outbound traffic to VMRC	1. Click the **Filter** icon in the **Name** column. 2. To display the VMRC proxy parameter, in the text box, enter `config.mksdevproxy.writethrottler` and close the dialog box. 3. In the **Value** text box, enter the outbound bandwidth limit in KBps.

5. Click **Save**.

Answer Virtual Machine Questions

Virtual machine questions are messages that are generated by vCenter Server. Virtual machine questions appear whenever the virtual machine needs user intervention to continue its operation. In most cases, virtual machine questions appear when you power on a virtual machine .

Verify that the virtual machine hardware version is 11 or later.

To save time and ensure the consistency of your virtual environment, you can apply the same answer to multiple or to all virtual machines that have the same pending question.

1. Navigate to a virtual machine with a question.
2. Right-click the virtual machine and select **Guest OS** > **Answer Question**.
   The **Answer Question** wizard opens.

3. In the **Answer Question** dialog box, select your answer.
4. Optional: Apply the selected answer to other virtual machines that have the same pending question.
   a) Click the **Select other virtual machines** hyperlink.
      A list of all virtual machines with the same pending question appears.
   b) Select the virtual machines to which to apply the answer.
5. Click **OK**.

Removing and Reregistering VMs and VM Templates

You can remove VMs and VM templates from the vCenter Server inventory or delete them from disk. If you only removed the VM from the inventory, you can add it back from the datastore.

Adding Existing Virtual Machines to vCenter Server

When you add a host to vCenter Server, it discovers all the virtual machines on that managed host and adds them to the vCenter Server inventory.

If a managed host is disconnected, the already discovered virtual machines continue to be listed in the inventory.

If a managed host is disconnected and reconnected, any changes to the virtual machines on that managed host are identified, and the vSphere Client updates the list of virtual machines. For example, if node3 is removed and node4 is added, the new list of virtual machines adds node4 and shows node3 as orphaned.

Remove VMs or VM Templates from vCenter Server or from the Datastore

You can temporarily remove a virtual machine or a VM template from vCenter Server or you can permanently delete it from the datastore.

Power off the virtual machine.

The process is the same for a virtual machine or a VM template:

- When you remove a virtual machine from the inventory, you unregister it from the host and vCenter Server, you do not delete it from the datastore. Virtual machine files remain at the same storage location and you can later re-register the virtual machine by using the datastore browser. This helps if you want to edit the virtual machine configuration file. It is also useful to temporarily remove a virtual machine when you have reached the maximum number of virtual machines that your license or hardware allows.
- If you no longer need a virtual machine and want to free up space on the datastore, you can remove the virtual machine from vCenter Server and delete all virtual machine files from the datastore, including the configuration file and virtual disk files.

Log in to the vSphere Client and perform the task:

Option	Description
Temporarily remove the virtual machine or VM template	1. Right-click the virtual machine. 2. Select **Remove From Inventory** and click **Yes**.
Permanently delete the virtual machine or VM template	1. Right-click the virtual machine. 2. Select **Delete from Disk** and click **Yes**.

Register a VM or VM Template with vCenter Server

If you removed a VM or VM template from vCenter Server but did not delete it from disk, you can return it to the vCenter Server inventory by registering it with the vCenter Server.

1. In the vSphere Client inventory, right-click the datastore on which the virtual machine configuration file is stored and select **Register VM**.
2. Browse to, select the virtual machine configuration (`.vmx`) file or the VM template configuration file (`.vmtx` file) and click **OK**.

   The **Register Virtual Machine** wizard opens.
3. On the Select a name and folder page, use the existing name or type a new name, select a datacenter or folder location and click **Next**.
4. Select a resource pool in which to run the virtual machine and click **Next**.
5. On the Ready to complete page, review your selections and click **Finish**.

Managing Virtual Machine Templates

After you clone a virtual machine to a template, you can perform different operation with the template. You can rename the template, delete it from the vCenter Server inventory, or delete it from the disk. You can also register the template with vCenter Server.

Change the Template Name

If you move a template to another host or datacenter folder, you can change the template name to make it unique in that folder.

1. Right-click the template and select **Rename**.
2. Enter a new name and click **OK**.

Deleting Templates

You can delete a template by removing it from the inventory or deleting the template from the disk. If you remove the template from the inventory, it remains on the disk and can be reregistered with vCenter Server to restore it to the inventory.

Remove Templates from the Inventory

If a template has become outdated and you no longer use it in your environment, you can remove it from the inventory. Removing a template unregisters it from the vCenter Server inventory, but it is not removed from the datastore. The template remains at the same storage location, and you can use the datastore browser to re-register the template at a later time. You can later decide to update the template rather than create one.

1. Click the template and select **Remove from Inventory**.
2. Click **Yes** to confirm removing the template from the vCenter Server database.

   The template is unregistered from the vCenter Server inventory.

Delete a Template from the Disk

If you no longer need a template or need to free up disk space, you can remove it from the disk. Templates that you delete are permanently removed from the system.

You cannot recover a template that you delete from the disk.

1. Right-click the template and select **Delete from Disk**.
2. Click **Yes** to confirm removing the template from the datastore.

Reregister Templates

Templates can become unregistered from vCenter Server if they are removed from the inventory or if the hosts with which they are associated are removed from vCenter Server and then readded.

1. In the vSphere Client, navigate to the datastore that contains the template.
2. Select the datastore and click the **Files** tab.
3. Locate the template folder and click it to display the template files.
4. Select the `.vmtx` file and click the **Register VM** icon.
   The **Register VM Template** wizard opens.
5. On the Select a name and folder page, specify a name and location for the template and click **Next**.
6. On the Select a compute resource page, select a host or cluster on which to store the template and click **Next**.
7. On the Ready to complete page, review your selections and click **Finish**.
8. Optional: To verify that the template is reregistered, check the host or cluster inventory.

Inventory Object	Steps
Host	Browse to the host. On the **VMs** tab, click **VM Templates**.
Cluster	On the **VMs** tab, click **VM Templates**.

The template is registered to the host. You can view the template by clicking on the host's **VM Templates**.

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. When you take a snapshot of a virtual machine, an image of the virtual machine in a given state is copied and stored. Snapshots are useful when you want to revert repeatedly to a virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking a snapshot of a VM for each member of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before you change a virtual machine.

Several operations for creating and managing virtual machine snapshots and snapshot trees are available in the vSphere Client. These operations enable you to create snapshots, revert any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create snapshot trees where you save the virtual machine state at any specific time so that you can revert that virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes the disks added or changed after you take the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.

The Snapshot Hierarchy

The vSphere Client presents the snapshot hierarchy as a tree with one or more branches. Snapshots in the hierarchy have parent to child relationships. In linear processes, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshot. Each parent snapshot can have more than one child. You can revert to the current parent snapshot or to any parent or child snapshot in the snapshot tree and create more snapshots from that snapshot. Each time you revert a snapshot and take another snapshot, a branch (child snapshot) is created.

Parent Snapshots	The first virtual machine snapshot that you create is the base parent snapshot. The parent snapshot is the most recently saved version of the current state of the virtual machine. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base `.vmdk` file. The parent snapshot is always the snapshot that appears immediately above the **You are here** icon in the Snapshot Manager. If you revert a snapshot, that snapshot becomes the parent of the **You are here** current state. **Note:** The parent snapshot is not always the snapshot that you took most recently.
Child Snapshots	A snapshot of a virtual machine taken after the parent snapshot. Each child snapshot contains delta files for each attached virtual disk, and optionally a memory file that points from the present state of the virtual disk (You are here). Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.

The relationship of parent and child snapshots can change if you have multiple branches in the snapshot tree. A parent snapshot can have more than one child. Many snapshots have no children.

CAUTION: Do not manually manipulate individual child disks or any of the snapshot configuration files because doing so can compromise the snapshot tree and result in data loss. This restriction includes disk resizing and making modifications to the base parent disk by using the `vmkfstools` command.

Snapshot Behavior

Taking a snapshot preserves the disk state at a specific time by creating a series of delta disks for each attached virtual disk or virtual RDM and optionally preserves the memory and power state by creating a memory file. Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings.

Each snapshot creates an additional delta `.vmdk` disk file. When you take a snapshot, the snapshot mechanism prevents the guest operating system from writing to the base `.vmdk` file and instead directs all writes to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the previous snapshot. If more than one snapshot exists, delta disks can represent the difference between each snapshot. Delta disk files can expand quickly and become as large as the entire virtual disk if the guest operating system writes to every block of the virtual disk.

Snapshot Files

When you take a snapshot, you capture the state of the virtual machine settings and the virtual disk. If you are taking a memory snapshot, you also capture the memory state of the virtual machine. These states are saved to files that reside with the virtual machine's base files.

Snapshot Files

A snapshot consists of files that are stored on a supported storage device. A Take Snapshot operation creates `.vmdk`, `-delta.vmdk`, `.vmsd`, and `.vmsn` files. By default, the first and all delta disks are stored with the base `.vmdk` file. The `.vmsd` and `.vmsn` files are stored in the virtual machine directory.

Delta disk files	A `.vmdk` file to which the guest operating system can write. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that the previous snapshot was taken. When you take a snapshot, the state of the virtual disk is preserved, the guest operating system stops writing to it, and a delta or child disk is created. A delta disk has two files. One is a small descriptor file that contains information about the virtual disk, such as geometry and child-parent relationship information. The other one is a corresponding file that contains the raw data. The files that make up the delta disk are called child disks or redo logs.
Flat file	A `-flat.vmdk` file that is one of two files that comprises the base disk. The flat disk contains the raw data for the base disk. This file does not appear as a separate file in the Datastore Browser.
Database file	A `.vmsd` file that contains the virtual machine's snapshot information and is the primary source of information for the Snapshot Manager. This file contains line entries, which define the relationships between snapshots and between child disks for each snapshot.
Memory file	A `.vmsn` file that includes the active state of the virtual machine. Capturing the memory state of the virtual machine lets you revert to a turned on virtual machine state. With nonmemory snapshots, you can only revert to a turned off virtual machine state. Memory snapshots take longer to create than nonmemory snapshots. The time the ESXi host takes to write the memory onto the disk depends on the amount of memory the virtual machine is configured to use.

A **Take Snapshot** operation creates `.vmdk`, `-delta.vmdk`, `vmsd` or `-sesparse.vmdk`, and `vmsn` files.

SEsparse is a default format for all delta disks on the VMFS6 datastores.

File	Description
vmname-*number*.vmdk, *vmname*-*number*-delta.vmdk, *vmname*-*number*-sesparse.vmdk	Snapshot file that represents the difference between the current state of the virtual disk and the state that existed at the time the previous snapshot was taken.

File	Description
	The filename uses the following syntax, `S1vm-000001.vmdk` where `S1vm` is the name of the virtual machine and the six-digit number, `000001`, is based on the files that already exist in the directory. The number does not consider the number of disks that are attached to the virtual machine.
vmname`.vmsd`	Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.
vmname`-.Snapshot`*number*`.vmsn`	Memory state of the virtual machine at the time you take the snapshot. The filename uses the following syntax, `S1vm.snapshot1.vmsn` , where `S1vm` is the virtual machine name, and `snapshot1` is the first snapshot. **Note:** A `.vmsn` file is created each time you take a snapshot, regardless of the memory selection. A `.vmsn` file without memory is much smaller than one with memory.

Snapshot Limitations

Snapshots can affect the virtual machine performance and do not support some disk types or virtual machines configured with bus sharing. Snapshots are useful as short-term solutions for capturing point-in-time virtual machine states and are not appropriate for long-term virtual machine backups.

- VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.
- Virtual machines with independent disks must be powered off before you take a snapshot.
- Starting with ESXi 7.0 Update 3l, you can take a memory snapshot of a virtual machine with an independent disk only to analyze the guest operating system behavior of a virtual machine. You cannot use such snapshots for virtual machine backups because restoring this type of snapshots is unsupported.
- Quiesced snapshots require VMware Tools installation and guest operating system support.
- Snapshots are not supported with PCI vSphere DirectPath I/O devices.
- VMware does not support snapshots of virtual machines configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine currently has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.
- Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost. Also, large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected if there is hardware failure.
- Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot. Also, you might see a delay in the amount of time it takes the virtual machine to power on. Do not run production virtual machines from snapshots on a permanent basis.

Managing Snapshots

You can view and manage all snapshots for an active virtual machine. You can review the snapshots information, revert to the latest snapshot, change the name and description, or delete a snapshot.

You can manage the snapshots when you select a virtual machine in the inventory and click the **Snapshots** tab.

The snapshot tree displays all snapshots of the virtual machine and the power state of the virtual machine when a snapshot was taken. The detailed information region contains the snapshot name and description, time of creation, and

the disk space. You can also see whether you took a snapshot of the virtual machine memory and if you quiesced the guest file system.

The **You are here** pin represents the current and active state of the virtual machine and it is always visible.

Taking Snapshots of a Virtual Machine

You can take one or more snapshots of a virtual machine to capture the settings state, disk state, and memory state at different specific times. When you take a snapshot, you can also quiesce the virtual machine files and exclude the virtual machine disks from snapshots.

When you take a snapshot, other activity that is occurring in the virtual machine might affect the snapshot process when you revert to that snapshot. The best time to take a snapshot from a storage perspective, is when you are not incurring a large I/O load. The best time to take a snapshot from a service perspective is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails. Depending on the task that you are performing, you can create a memory snapshot or you can quiesce the file system in the virtual machine.

Memory Snapshots	The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state. When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.
Quiesced Snapshots	When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files. If the virtual machine is powered off or VMware Tools is not available, the `Quiesce` parameter is not available. You cannot quiesce virtual machines that have large capacity disks.

Important: Do not use snapshots as your only backup solution or as a long-term backup solution.

Change Disk Mode to Exclude Virtual Disks from Snapshots

You can set a virtual disk to independent mode to exclude the disk from any snapshots taken of its virtual machine.

Power off the virtual machine and delete any existing snapshots before you change the disk mode. Deleting a snapshot involves committing the existing data on the snapshot disk to the parent disk.

Required privileges:

- **Virtual machine** > **Snapshot management** > **Remove Snapshot**
- **Virtual machine** > **Configuration** > **Modify device settings**

Note: An independent disk does not participate in virtual machine snapshots. That is, the disk state is independent of the snapshot state and creating, consolidating, or reverting to snapshots does not have effect on the disk.

Starting with ESXi 7.0 Update 3l, you can take a memory snapshot of a virtual machine with an independent disk only to analyze the guest operating system behavior of a virtual machine. You cannot use such snapshots for virtual machine backups because restoring this type of snapshots is unsupported.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Hard disk**, and select an independent disk mode option.

Option	Description
Dependent	Dependent mode is the default disk mode. When you take a snapshot of a virtual machine, dependent disks are included in the snapshot. When you revert to the previous snapshot, all data are reverted to the point of taking a snapshot.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk even if you revert a snapshot. When you power off or reset a virtual machine, the disk and all its snapshots are preserved.
Independent - Nonpersistent	Disks in nonpersistent mode behave like read-only disks. Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset the virtual machine, or when you delete a snapshot.

3. Click **OK**.

Take a Snapshot of a Virtual Machine

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. If you are suspending a virtual machine, wait until the suspend operation finishes before you take a snapshot.

- If you are taking a memory snapshot of a virtual machine that has multiple disks in different disk modes, verify that the virtual machine is powered off. For example, if you have a special purpose configuration that requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.
- To capture the memory state of the virtual machine, verify that the virtual machine is powered on.
- To quiesce the virtual machine files, verify that the virtual machine is powered on and that VMware Tools is installed.
- Verify that you have the **Virtual machine** > **Snapshot management** > **Create snapshot** privilege on the virtual machine.

When you create a memory snapshot, the snapshot captures the state of the virtual machine memory and the virtual machine power settings. When you capture the virtual machine memory state, the snapshot operation takes longer to complete. You might also see a momentary lapse in response over the network.

When you quiesce a virtual machine, VMware Tools quiesces the file system in the virtual machine. The quiesce operation pauses or alters the state of running processes on the virtual machine, especially processes that might modify information stored on the disk during a revert operation.

Application-consistent quiescing is not supported for virtual machines with IDE or SATA disks.

Note: If you take a snapshot of a Dynamic Disk (a Microsoft-specific disk type), the snapshot technology preserves the quiesce state of the file system, but does not preserve the quiesce state of the application.

1. In the , navigate to a virtual machine and click the **Snapshots** tab.
2. Click **Take Snapshot**.
   The **Take snapshot** dialog box opens.
3. Enter a name for the snapshot.
4. Optional: Enter a description for the snapshot.
5. Optional: To capture the memory of the virtual machine, select the **Snapshot the virtual machine's memory** check box.
6. Optional: To pause running processes on the guest operating system so that file system contents are in a known consistent state when you take a snapshot, select the **Quiesce guest file system (requires VMware Tools)** check box.
   You can quiesce the virtual machine files only when the virtual machine is powered on and the **Snapshot the virtual machine's memory** check box is deselected.
   For more information about the virtual machine behavior when you quiesce a virtual machine, see the KB article https://kb.vmware.com/s/article/5962168.
7. Click **Create**.

Revert a Virtual Machine Snapshot

To return a virtual machine to its original state, or to return to another snapshot in the snapshot hierarchy, you can use the revert options.

Verify that you have the**Virtual machine** > **Snapshot management** > **Revert to snapshot** privilege on the virtual machine.

When you revert a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in when you took the snapshot. You can revert any snapshot in the snapshot tree and make that snapshot the parent snapshot of the current state of the virtual machine. Subsequent snapshots from this point create a new branch of the snapshot tree.

Restoring snapshots has the following effects:

- The current disk and memory states are discarded, and the virtual machine reverts to the disk and memory states of the parent snapshot.
- Existing snapshots are not removed. You can revert those snapshots at any time.
- If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot.

Table 168: Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Note: vApp metadata for virtual machines in vApps does not follow the snapshot semantics for the virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

When you revert to a snapshot, disks that you added or changed after the snapshot was taken are reverted to the snapshot point. For example, when you take a snapshot of a virtual machine, add a disk, and revert the snapshot, the added disk is removed.

Independent disks are also removed when you revert to a snapshot that was taken before the disk was added. If the latest snapshot includes an independent disk, its contents do not change when you revert to that snapshot.

1. To revert a snapshot, navigate to a virtual machine in the vSphere Client inventory and click the **Snapshots** tab.
2. Navigate to a snapshot in the snapshot tree, click **Revert**, and click the **Revert** button.

Delete a Snapshot

Deleting a snapshot permanently removes the snapshot from the snapshot tree. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk. You can delete a single snapshot or all snapshots in a snapshot tree.

- Familiarize yourself with the delete and delete all actions and how they affect virtual machine performance.
- Required Privilege: **Virtual machine** > **Snapshot management** > **Remove Snapshot** on the virtual machine.

Deleting a snapshot does not change the virtual machine or other snapshots. Deleting a snapshot consolidates the changes between snapshots and previous disk states. Then it writes all the data from the delta disk that contains the information about the deleted snapshot to the parent disk. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

To delete a snapshot, a large amount of information must be read and written to a disk. This process can reduce the virtual machine performance until the consolidation is complete. Consolidating snapshots removes redundant disks, which improves the virtual machine performance and saves storage space. The time to delete snapshots and consolidate the snapshot files depends on the amount of data that the guest operating system writes to the virtual disks after you take the last snapshot. If the virtual machine is powered on, the required time is proportional to the amount of data the virtual machine is writing during consolidation.

Failure of disk consolidation can reduce the performance of virtual machines. You can check whether any virtual machines require separate consolidation operations by viewing a list. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see Consolidate Snapshots.

Delete	Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. This option writes disk changes that occur between the state of the snapshot and the previous disk state to the parent snapshot. **Note:** Deleting a single snapshot preserves the current state of the virtual machine and does not affect any other snapshot. You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.
Delete All	Use the **Delete All** option to delete all snapshots from the snapshot tree. The **Delete all** option consolidates and writes the changes that occur between snapshots and the previous delta disk states to the base parent disk. It then merges them with the base virtual machine disk.

To prevent snapshot files from merging with the parent snapshot if, for example, an update or installation fails, first use the **Revert** button to revert to a previous snapshot. This action invalidates the snapshot delta disks and deletes the memory file. You can then use the **Delete** option to remove the snapshot and any associated files.

CAUTION: Use care when you delete snapshots. You cannot revert a deleted snapshot. For example, you might want to install several browsers, a, b, and c, and capture the virtual machine state after you install each browser. The first, or base snapshot, captures the virtual machine with browser a and the second snapshot captures browser b. If you revert the base snapshot that includes browser a and take a third snapshot to capture browser c, and delete the snapshot that contains browser b, you cannot return to the virtual machine state that includes browser b.

To delete snapshots from a snapshot tree, navigate to a virtual machine in the vSphere Client inventory and click the **Snapshots** tab.

Option	Action
Delete a single snapshot	1. Navigate to and select a snapshot in the snapshots tree. 2. Click **Delete** and click the **Delete** button. The snapshot data is consolidated to the parent snapshot and the selected snapshot is removed from the snapshot tree.
Delete all snapshots	1. Click **Delete All** and click the **Delete all** button. All immediate snapshots before the **You are here** current state are consolidated to the base parent disk. All existing snapshots are removed from the snapshot tree and the virtual machine.

Consolidate Snapshots

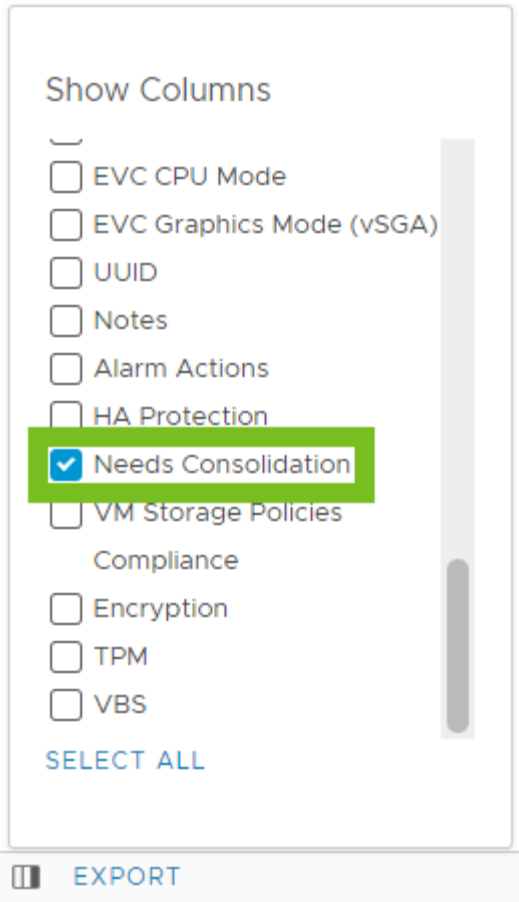
The presence of redundant delta disks can adversely affect the virtual machine performance. You can combine such disks without violating a data dependency. After consolidation, redundant disks are removed, which improves the virtual machine performance and saves storage space.

Required privilege: **Virtual machine** > **Snapshot management** > **Remove Snapshot**

Snapshot consolidation is useful when snapshot disks fail to compress after a **Revert**, **Delete**, or **Delete all** operation. This might happen, for example, if you delete a snapshot but its associated disk does not commit back to the base disk.

1. Navigate to a virtual machine in the vSphere Client inventory and click the **Snapshots** tab.
2. Perform the necessary snapshot operations.
   If the virtual machine snapshot files must be consolidated, the **Consolidation is required** message appears.
3. Click the **Consolidate** button.
   The **Consolidate** dialog box appears.

4. Click **OK**.
5. To verify that the consolidation is successful, check the **Needs Consolidation** column.
   a) Navigate to an inventory object that contains a list of virtual machines, for example a vCenter Server instance, a host, or a cluster.
   b) Click the **VMs** tab and click **Virtual Machines**.
   c) Click .
      The **Show Columns** window appears.



   d) Select **Needs Consolidation**.
      A `Yes` status indicates that the snapshot files for the virtual machine must be consolidated. A `Not Required` status indicates that the files are consolidated.

Enhanced vMotion Compatibility as a Virtual Machine Attribute

Enhanced vMotion Compatibility (EVC) is a cluster feature that ensures CPU compatibility between hosts in a cluster, so that you can seamlessly migrate virtual machines within the EVC cluster. You can also activate, deactivate, or change the EVC mode at the virtual machine level. The per-VM EVC feature facilitates the migration of the virtual machine beyond the cluster and across vCenter Server systems and data centers that have different processors.

Starting with vSphere 7.0 Update 1, you can take advantage of the EVC feature for Virtual Shared Graphics Acceleration (vSGA). vSGA allows multiple virtual machines to share GPUs installed on ESXi hosts and leverage the 3D graphics acceleration capabilities.

The EVC mode of a virtual machine is independent from the EVC mode defined at the cluster level. The cluster-based EVC mode limits the CPU features a host exposes to virtual machines. The per-VM EVC mode determines the set of host CPU features that a virtual machine requires to power on and migrate.

By default, when you power on a newly created virtual machine, it inherits the feature set of its parent EVC cluster or host. However, you can change the EVC mode for each virtual machine separately. You can raise or lower the EVC mode of a virtual machine. Lowering the EVC mode increases the CPU compatibility of the virtual machine. You can also use the API calls to customize the EVC mode further.

Cluster-Level EVC and Per-VM EVC

There are several differences between the way the EVC feature works at the host cluster level and at the virtual machine level.

- Unlike cluster-based EVC, you can change the per-VM EVC mode only when the virtual machine is powered off.
- With cluster-based EVC, when you migrate a virtual machine out of the EVC cluster, a power cycle resets the EVC mode that the virtual machine has. With Per-VM EVC, the EVC mode becomes an attribute of the virtual machine. A power cycle does not affect the compatibility of the virtual machine with different processors.
- When you configure EVC at the virtual machine level, the per-VM EVC mode overrides cluster-based EVC. If you do not configure per-VM EVC, when you power on the virtual machine, it inherits the EVC mode of its parent EVC cluster or host.
- If a virtual machine is in an EVC cluster and the per-VM EVC is also enabled, the EVC mode of the virtual machine cannot exceed the EVC mode of the EVC cluster in which the virtual machine runs. The baseline feature set that you configure for the virtual machine cannot contain more CPU features than the baseline feature set applied to the hosts in the EVC cluster. For example, if you configure a cluster with the Intel "Merom" Generation EVC mode, you should not configure a virtual machine with any other Intel baseline feature set. All other sets contain more CPU features than the Intel "Merom" Generation feature set and as a result of such configuration, the virtual machine fails to power on.

Compatibility and Requirements

The per-VM EVC feature has the following requirements.

Compatibility	Requirement
Host compatibility	
vCenter Server compatibility	
Virtual machine compatibility	Virtual hardware version 14 or later.

To check EVC support for a specific processor or server model, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.

Configure the EVC Mode of a Virtual Machine

Per-VM EVC is deactivated by default. You can activate, deactivate, and change the EVC mode of a virtual machine to ensure its seamless migration across clusters, vCenter Server systems, and data centers that have different processors.

Power off the virtual machine.

To check what the EVC mode of a virtual machine is, see Determine the EVC Mode of a Virtual Machine.

1. Navigate to a virtual machine in the vCenter Server inventory.
2. On the **Configure** tab, select **VMware EVC**.
   The pane shows details about the EVC mode of the virtual machine and CPUID details.

   Important: For newly created virtual machines, the EVC mode that shows in the **VMware EVC** pane is deactivated.

   For powered off virtual machines, the **VMware EVC** pane always shows the EVC status defined at the virtual machine level.

   For powered on virtual machines with per-VM EVC activated, the VMware EVC pane shows the EVC status defined at the virtual machine level.

   For powered on virtual machines with per-VM EVC deactivated, the VMware EVC pane shows the EVC mode that the virtual machine inherits from its parent EVC cluster or host.
3. Click the **Edit** button.
   The **Change EVC Mode** dialog box opens.
4. In the **Change EVC Mode** dialog box, select whether to activate or deactivate EVC.

Option	Description
Disable EVC	The EVC feature is deactivated for the virtual machine. When you power on the virtual machine, it inherits the feature set of its parent EVC cluster or host.
Enable EVC for AMD hosts	The EVC feature is activated for AMD hosts.
Enable EVC for Intel hosts	The EVC feature is activated for Intel hosts.
Custom	This option is visible only if you have customized the EVC mode of the virtual machine through the API calls.

5. Optional: From the **CPU Mode** drop-down menu, select a baseline CPU feature set.

   Important: If the virtual machine is in an EVC cluster and the per-VM EVC mode exceeds the EVC mode for the cluster, the virtual machine fails to power on. The baseline CPU feature set for the virtual machine must not contain more CPU features than the baseline CPU feature set of the cluster.
6. Optional: From the **Graphics Mode (vSGA)** drop-down menu, select a baseline graphics feature set.

Option	Description
Baseline Graphics	Applies the Baseline Graphics feature set that includes features through Direct3D 10.1/OpenGL 3.3. **Note:** To configure the vSGA mode to apply the Baseline Graphics set that includes features through Direct3D 10.1/ OpenGL 3.3, the virtual machine must be compatible with ESXi 7.0 Update 1 or earlier.
D3D 11.0 class features	Applies the baseline graphics feature set that includes features through Direct3D 11.0/OpenGL 4.1 **Note:** To configure the vSGA mode to apply the Baseline Graphics set that includes features through Direct3D 11.0/ OpenGL 4.1, verify that the virtual machine is compatible with ESXi 7.0 Update 2 or later and has installed VMware Tools 11.1.5 or later.

Option	Description
	To power on a virtual machine, configured with Direct3D 11.0/ OpenGL 4.1, verify that the ESXi host graphics hardware is available.

7. Click **OK**.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU and graphics features that a host must have in order for the virtual machine to migrate to that host and power on. The EVC mode of a virtual machine is independent from the EVC mode that you configure for the cluster in which the virtual machine runs.

The EVC mode of a virtual machine is determined when the virtual machine powers on. At power-on, the virtual machine also determines the EVC mode of the cluster in which it runs. If the EVC mode of a running virtual machine or the entire EVC cluster is raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not use any CPU features exposed by the new EVC mode until the virtual machine is powered off and powered on again.

For example, you create an EVC cluster that contains hosts with Intel processors and you set the EVC mode to Intel "Merom" Generation (Xeon Core 2). When you power on a virtual machine in this cluster, it runs in the Intel Merom Generation (Xeon Core 2) EVC mode. If you raise the EVC mode of the cluster to Intel "Penryn" Generation (Xeon 45 nm Core 2), the virtual machine retains the lower Intel "Merom" Generation (Xeon Core 2) EVC mode. To use the feature set of the higher EVC mode, such as SSE4.1, the virtual machine must be powered off and powered on again.

1. Navigate to a cluster or a host in the vCenter Server inventory.
2. Click the **VMs** > **Virtual Machines** tab.

   A list of all virtual machines in the selected cluster or on the selected host appears.

3. To verify the status of the CPU mode, check the **EVC CPU Mode** column.
   a) If the column is not visible, click the **Pick columns** icon ( ) at the bottom left corner of the **Virtual Machines** table.
      The **Show Columns** pop-up appears.
   b) To show the **EVC CPU Mode** column, locate and select the respective check box from the list.

   The **EVC CPU Mode** column shows the CPU modes of all virtual machines in the cluster or on the host.

   Important: For each virtual machine, the **EVC CPU Mode** column displays the EVC mode defined at the virtual machine level.

   However, if you do not configure per-VM EVC for a virtual machine, the virtual machine inherits the EVC mode of its parent cluster or host. As a result, for all virtual machines that do not have per-VM EVC configured, the **EVC CPU Mode** column displays the inherited EVC mode of the parent host or cluster.

   If the virtual machine is in an EVC cluster, the EVC mode that you see in the **EVC CPU Mode** column is defined in the following manner.

   - When the virtual machine is powered on, the **EVC CPU Mode** column displays either the per-VM EVC mode, or the cluster-level EVC mode.

Per-VM EVC	Cluster-Level EVC	EVC Mode for the Virtual Machine
Activated	Activated	Enabled. The **EVC CPU Mode** column displays the EVC mode of the virtual machine.
Deactivated	Activated	Enabled. The **EVC CPU Mode** column displays the EVC mode of the EVC cluster.

   - When the virtual machine is powered off, the **EVC CPU Mode** column displays the per-VM EVC mode. If per-VM EVC is disabled, the **EVC CPU Mode** column for the virtual machine is empty.

   When the virtual machine is not in an EVC cluster and per-VM EVC is not configured, the EVC mode that you see in the **EVC CPU Mode** column is defined in the following manner.

   - When the virtual machine is powered on, the **EVC CPU Mode** column displays the EVC mode of the parent host.
   - When the virtual machine is powered off, the **EVC CPU Mode** column is empty.

4. To verify the status of the graphics mode, check the **EVC Graphics Mode (vSGA)** column.
   a) If the column is not visible, click the **Pick columns** icon ( ) at the bottom left corner of the **Virtual Machines** table.
      The **Show Columns** pop-up appears.
   b) To show the **EVC Graphics Mode (vSGA)** column, locate and select the respective check box from the list.

   The **EVC Graphics Mode (vSGA)** column displays the baseline graphics features set. To view the baseline graphics, you must enable **3D graphics** in the virtual machine.

   For information about configuring 3D graphics in a virtual machine, see the *vSphere Virtual Machine Administration* guide.

Virtual Machine Storage DRS Rules

The Storage DRS rules that you define at the virtual machine level function in the same way as the affinity and anti-affinity rules that you define at the datastore cluster level. Virtual machine Storage DRS rules define whether virtual machine

hard disks are placed and kept on the same datastore or on different datastores within a datastore cluster. You can also create Storage DRS rules that place and keep all virtual disks of certain virtual machines on different datastores within a datastore cluster.

In the vSphere Client, you can create, edit, and delete Storage DRS rules.

VMDK Affinity Rules

By default, all virtual machine hard disks are kept together on the same datastore within a datastore cluster that has Storage DRS enabled. That is, VMDK affinity rules are enabled by default for all virtual machines that are in a datastore cluster. You can override that rule for the datastore cluster or for individual virtual machines.

Storage DRS Anti-Affinity Rules

You can also create anti-affinity rules to place certain virtual hard disks or virtual machines on different datastores and keep them separated.

- VMDK anti-affinity rules ensure that two or more virtual hard disks of a single virtual machine are placed and kept on different datastores within the datastore cluster.
- VM anti-affinity rules ensure that all the virtual hard disks of two or more virtual machines are placed and kept on different datastores within the datastore cluster.

For more information about Storage DRS, see the *vSphere Resource Management* documentaion.

Add a VMDK Affinity Rule

Create a VMDK affinity rule to place and keep all virtual disks of a virtual machine on the same datastore within a datastore cluster.

1. Navigate to a virtual machine in the inventory.
2. On the **Configure** tab, expand **Settings** and click **VM SDRS Rules**.
3. Click the **Add** button.

   The **Add SDRS rule** dialog box opens.
4. From the **Type** drop-down menu, select **VMDK affinity**.
5. From the **Datastore cluster** drop-down menu, select the datastore cluster where you want to keep the virtual machine disks.

   A datastore cluster is visible in the list only if the virtual machine configuration file or at least one of the virtual hard disks is placed on a datastore within the datastore cluster.
6. Optional: Deselect the **Keep VMDKs together** to create a rule that places and keeps the virtual hard disks on different datastores.

   If you leave the check box selected, the rule that you create is the same as the default Storage DRS rule that operates at the datastore cluster level.

   Deselecting the check box creates a Storage DRS rule that overrides the default VMDK affinity rule for the datastore cluster.
7. Click **OK**.

An Intra-VM Affinity rule is created that keeps VMDKs together. That is, all virtual hard disks of the selected virtual machine are placed and kept together on the same datastore within the datastore cluster.

Add a VMDK Anti-Affinity Rule

Create a VMDK anti-affinity rule to place and keep certain virtual hard disks of a virtual machine on different datastores within the datastore cluster.

When you create an anti-affinity rule, it applies to those of the virtual machine's hard disks that are on datastores within the selected datastore cluster. Anti-affinity Storage DRS rules operate during migrations that Storage DRS initiates or recommends, but they do not operate when the user initiates a migration.

1. Navigate to a virtual machine in the inventory.
2. On the **Configure** tab, expand **Settings** and click **VM SDRS Rules**.
3. Click the **Add** button.
   The **Add SDRS rule** dialog box opens.
4. From the **Type** drop-down menu, select **VMDK anti-affinity**.
5. In the **Rule name** text box, enter a name for the rule.
6. From the **Datastore cluster** drop-down menu, select the datastore cluster where the anti-affinity rule will operate.
   All virtual hard disks that are placed on datastores within the selected datastore cluster appear at the bottom of the dialog box.
7. Select the virtual hard disks to which the anti-affinity rule applies.
8. Optional: Deselect the **Enable the rule** check box.
   Deselecting the **Enable the rule** check box deactivates the rule. You can still create the rule, but after creation the rule is not applied to the selected virtual hard disks.
9. Click **OK**.

A VMDK anti-affinity rule is created. If the rule is enabled, all selected virtual hard disks are placed and kept on different datastores within the datastore cluster.

Add a VM Anti-Affinity Rule

Create a VM anti-affinity rule to place and keep all virtual hard disks of selected virtual machines on different datastores within the datastore cluster.

1. Navigate to a virtual machine in the inventory.
2. On the **Configure** tab, expand **Settings** and click **VM SDRS Rules**.
3. Click the **Add** button.
   The **Add SDRS rule** dialog box opens.
4. From the **Type** drop-down menu, select **VM anti-affinity**.
5. In the **Rule name** text box, enter a name for the rule.
6. From the **Datastore cluster** drop-down menu, select the datastore cluster where the anti-affinity rule will operate.
7. From the list of virtual machines at the bottom of the dialog box, select the virtual machines to which the anti-affinity rule applies.
   You can add or remove virtual machines to the list.

8. Optional: Deselect the **Enable the rule** check box.

   The rule is enabled by default.

   Deselecting the **Enable the rule** check box deactivates the rule. If an existing rule is deactivated, it is not applied to the virtual machine.

9. Click **OK**.

A VM anti-affinity rule is created. If the rule is enabled, all virtual hard disks of the selected virtual machines are placed and kept on different datastores within the datastore cluster.

Distributing Content with GuestStore

The GuestStore feature provides an easy and flexible mechanism to maintain and distribute various content types across multiple virtual machines on multiple ESXi hosts at the same time. By using the GuestStore framework, you can make sure that the distributed content is always consistent and you can improve the content management in your environment.

As a vSphere administrator, after you configure GuestStore on an ESXi host, the virtual machines on the host can start accessing the GuestStore content immediately.

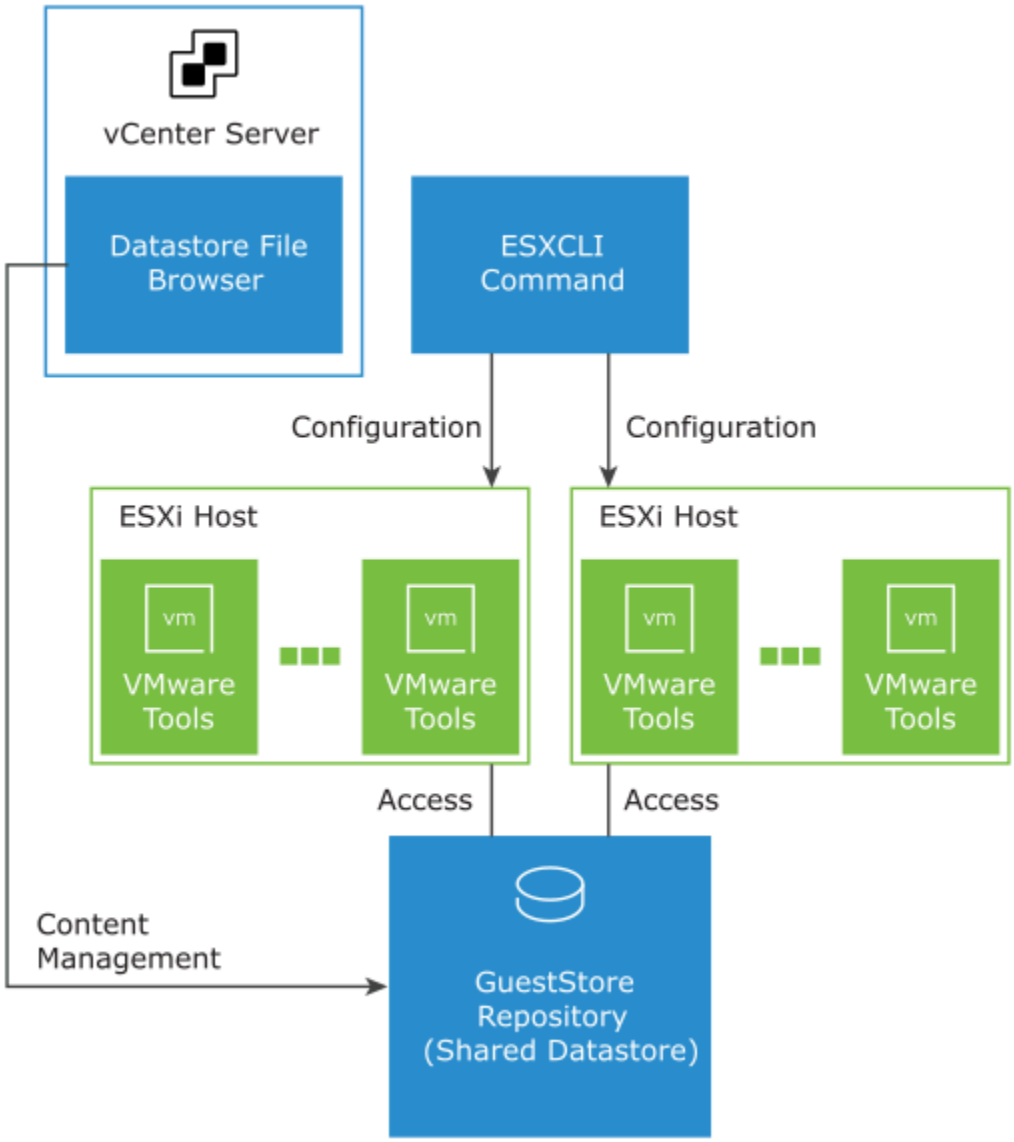
The GuestStore content consists of:

- Binary files that contain updates for VMware Tools and VMware agents.
- Scripts that are either provided by VMware or are custom scripts.
- Configuration files of VMware Tools and VMware agents.

With GuestStore you can:

- Maintain the content on a datastore, that is called a GuestStore repository.
- Fetch and distribute VMware Tools and VMware agent updates.
- Distribute configurations for VMware Tools and different VMware agents.
- Distribute a custom content - custom scripts, agents, and configuraton files.

For example, by importing VMware Tools in the GuestStore repository, you can schedule an automated VMware Tools upgrade at the next reboot of the virtual machine. From the GuestStore repository, you can also perform VMware Tools upgrade for particular virtual machines when necessary.



By using vSphere Client, you can configure a GuestStore repository on a shared datastore of an ESXi host. You perform the configuration by using ESXCLI. You manage the contents of your datastore by using the datastore file browser, or, if you use an NFS datastore, you can mount the datastore to any NFS client machine.

By using a PowerCLI script, you can configure multiple hosts or a cluster managed by a vCenter Server system.

To access the GuestStore contents, the virtual machine guest operating system uses a resource path. The path to the datastore contents must be the same as the resource path of the guest operating system. For example, to access the `/example/myrepository/bar` file in the GuestStore repository, the resource path in the guest operating system must be the same, that means `/example/myrepository/bar`.

Starting with vSphere 7.0 Update 2, you can download and extract the VMware Tools content under the GuestStore repository path. The GuestStore framework allows you, as a vSphere Client administrator, to distribute a configuration file or VMware agent to set of various guest operating systems. For information about configuring GuestStore for VMware Tools, see the *VMware Tools* documentation.

Requirements for GuestStore

To use GuestStore, your vSphere environment must meet the following requirements:

- Virtual machines with Windows guest operating systems must be running on ESXi 7.0 Update 2 and later and VMware Tools 11.2.5 and later versions.
- Virtual machines with Linux guest operating systems must be running on ESXi 7.0 Update 3 and later and VMware Tools 11.3.0 and later versions.
- The file that is distributed through GuestStore must be 512 MB or smaller.

Set the GuestStore Repository with ESXCLI

You can use ESXCLI commands to set the URL to the GuestStore repository and verify the configuration by retrieving the currently set URL.

1. Set the GuestStore repository URL.

   Note: The URL must point to a datastore path where GuestStore content is stored. The datastore path must be accessible to the ESXi host. If you want to set up a common GuestStore repository across multiple ESXi hosts, you should use a shared datastore path.

   ```
   esxcli system settings gueststore repository set --url "<datastore_path>"
   ```

   The following example contains a possible syntax for the datastore path.

   ```
   esxcli system settings gueststore repository set --url "ds:///vmfs/volumes/<datastore_uuid>/GuestStore"
   ```

2. Retrieve the GuestStore repository URL.

   ```
   esxcli system settings gueststore repository get
   ```

   You receive the currently set URL in the output.

   ```
   URL: <datastore_path>
   ```

Clear the GuestStore Repository Setting with ESXCLI

You can use ESXCLI commands to clear the GuestStore repository URL setting and verify that the URL is not set.

1. Clear the GuestStore repository URL setting.

   ```
   esxcli system settings gueststore repository set --url ""
   ```

2. Retrieve the GuestStore repository URL.

   ```
   esxcli system settings gueststore repository get
   ```

   You receive the URL information in the output.

   ```
   URL: <not set>
   ```

Migrating Virtual Machines

You can move virtual machines from one compute resource or storage location to another by using cold or hot migration. For example, with vSphere vMotion you can move powered on virtual machines away from a host to perform maintenance, to balance loads, to collocate virtual machines that communicate with each other, to move virtual machines apart to minimize fault domain, to migrate to new server hardware, and so on.

Moving a virtual machine from one inventory folder to another folder or resource pool in the same data center is not a form of migration. Unlike migration, cloning a virtual machine or copying its virtual disks and configuration file in the same vCenter Server system are procedures that create a new virtual machine. Cloning and copying a virtual machine in the same vCenter Server system are also not forms of migration.

By using migration, you can change the compute resource that the virtual machine runs on. For example, you can move a virtual machine from one host to another host or cluster.

To migrate virtual machines with disks larger than 2 TB, the source and destination ESXi hosts must be version 6.0 and later.

Depending on the power state of the virtual machine that you migrate, migration can be cold or hot.

Cold Migration	Moving a powered off or suspended virtual machine to a new host. Optionally, you can relocate configuration and disk files for powered off or suspended virtual machines to new storage locations. You can also use cold migration to move virtual machines from one virtual switch to another, and from one data center to another. You can perform cold migration manually or you can schedule a task.
Hot Migration	Moving a powered on virtual machine to a new host. Optionally, you can also move the virtual machine disks or folder to a different datastore. Hot migration is also called live migration or vSphere vMotion. With vSphere vMotion, you migrate the virtual machine without any interruption in its availability.

Depending on the virtual machine resource type, you can perform three types of migration.

Change compute resource only	Moving a virtual machine, but not its storage, to another compute resource, such as a host, cluster, resource pool, or vApp. You can move the virtual machine to another compute resource by using cold or hot migration. If you change the compute resource of a powered on virtual machine, you use vSphere vMotion.
Change storage only	Moving a virtual machine and its storage, including virtual disks, configuration files, or a combination of these, to a new datastore on the same host. You can change the datastore of a virtual machine by using cold or hot migration. If you move a powered on virtual machine and its storage to a new datastore, you use Storage vMotion.
Change both compute resource and storage	Moving a virtual machine to another host and at the same time moving its disk or virtual machine folder to another datastore. You can change the host and datastore simultaneously by using cold or hot migration.

In vSphere 6.0 and later, you can move virtual machines between vSphere sites by using migration between the following types of objects.

Migrate to another virtual switch	Moving the network of a virtual machine to a virtual switch of a different type. You can migrate virtual machines without reconfiguring the physical and virtual network. By using cold or hot migration, you can move the virtual machine from a standard to a standard or distributed switch, and from a distributed switch to another distributed switch. When you move a virtual machine network between distributed switches, the network configuration and policies that are associated with the network adapters of the virtual machine are transferred to the target switch.
Migrate to another data center	Moving a virtual machine to a different data center. You can change the data center of a virtual machine by using cold or hot migration. For networking in the target data center, you can select a dedicated port group on a distributed switch.
Migrate to another vCenter Server system	Moving a virtual machine to a different vCenter Server instance. You can move a virtual machine to a vCenter Server instance that is connected to the source vCenter Server instance through vCenter Enhanced Linked Mode. You can also move virtual machines between vCenter Server instances that are located across a long distance from each other.

Starting with vSphere 7.0 Update 1c, you can migrate workloads across vCenter Server systems by using Advanced Cross vCenter vMotion. You can initiate migration of workloads both from on-premise environments and from cloud environments. Advanced Cross vCenter vMotion does not depend on vCenter Enhanced Linked Mode or Hybrid Linked Mode and you can migrate virtual machines across vCenter Server systems in different vCenter Single Sign-On domains.

Starting with vSphere 7.0 Update 3, you can use the Advanced Cross vCenter vMotion feature to clone virtual machines across vCenter Server systems.

Virtual Machine Conditions and Limitations for vMotion

To migrate virtual machines with vMotion, the virtual machine must meet certain network, disk, CPU, USB, and other device requirements.

The following virtual machine conditions and limitations apply when you use vMotion:

- The source and destination management network IP address families must match. You cannot migrate a virtual machine from a host that is registered to vCenter Server with an IPv4 address to a host that is registered with an IPv6 address.
- Using 1 GbE network adapters for the vMotion network might result in migration failure, if you migrate virtual machines with large vGPU profiles. Use 10 GbE network adapters for the vMotion network.
- If virtual CPU performance counters are enabled, you can migrate virtual machines only to hosts that have compatible CPU performance counters.
- You can migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use the graphics renderer that is present on the destination host. The renderer can be the host CPU or a GPU graphics card. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU graphics card.
- Starting with vSphere 6.7 Update 1 and later, vSphere vMotion supports virtual machines with vGPU.
- vSphere DRS supports initial placement of vGPU virtual machines running vSphere 6.7 Update 1 or later without load balancing support.
- You can migrate virtual machines with USB devices that are connected to a physical USB device on the host. You must enable the devices for vMotion.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device that is not accessible on the destination host. For example, you cannot migrate a virtual machine with a CD drive backed by the physical CD drive on the source host. Disconnect these devices before you migrate the virtual machine.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device on the client computer. Disconnect these devices before you migrate the virtual machine.
- You can simultaneously migrate virtual machines at a certain network, host, and datastore resource cost. When a resource exceeds its maximum cost, new migration operations are queued until the required resources are available. See Limits on Simultaneous Migrations.

Migrate a Powered Off or Suspended Virtual Machine

You can use cold migration to move a virtual machine and its associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

-

- Required privilege: **Resource** > **Migrate powered off virtual machine**

1. Power off or suspend the virtual machine.
2. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
3. Select the migration type and click **Next**.

Option	Description
Change compute resource only	Move the virtual machine to another host.
Change storage only	Move the virtual machine's configuration file and virtual disks.
Change both compute resource and storage	Move the virtual machine to another host and move its configuration file and virtual disks.

4. If you change the compute resource of the virtual machine, select the destination compute resource for this virtual machine migration and click **Next**.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and DRS clusters with any level of automation. If a cluster has no DRS enabled, select a specific host in the cluster rather than selecting the cluster.

   Important:

   If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

   If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks will use the storage policy and datastore selected for the configuration files of the virtual machine.

   Important: Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and choose a destination host that is licensed to use PMem devices.

5. On the Select storage page, select the storage type for the virtual machine configuration files and all the hard disks.
   - If you select the **Standard** mode, all virtual disks are stored on a standard datastore.
   - If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.
   - If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.
6. Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual

Option	Action
	disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated

Option	Action
	at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned

Option	Action
	disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

7. Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

   Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

   Important: If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

8. Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. To deactivate Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Configure per disk**. **Note:** You can use the **Configure per disk** option to dowgrade from or upgrade to PMem storage.

Option	Action
	2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

9. Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

   You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

   You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

10. On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource

You can use the **Migration** wizard to migrate a powered-on virtual machine from one compute resource to another by using vMotion. To relocate only the disks of a powered-on virtual machine, migrate the virtual machine to a new datastore by using Storage vMotion.

Verify that your hosts and virtual machines meet the requirements for migration with vMotion with shared storage.

- Required privilege: **Resource** > **Migrate powered on virtual machine**

1. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
2. Click **Change compute resource only** and click **Next**.
3. Select a host, cluster, resource pool, or vApp to run the virtual machine, and click **Next**.

   Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and fully automated DRS clusters in the same or another vCenter Server system. If your target is a non-automated cluster, select a host within the non-automated cluster.

   Important:

   If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

   If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resources, so that all PMem hard disks remain stored on a

PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important: Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

4. Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

   You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

   You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

5. Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is

Option	Description
	not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

6. Review the page and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to New Storage

Migrate a virtual machine with Storage vMotion to relocate the configuration file and virtual disks while the virtual machine is powered on.

•

• Required privilege: **Resource** > **Migrate powered on virtual machine**

You can change the virtual machine host during a migration with Storage vMotion.

1. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
2. Click **Change storage only** and click **Next**.
3. Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not

Option	Action
	erased during creation. Instead, it is zeroed out on demand on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data

Option	Action
	remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the

Option	Action
	thin disk needs more space later, it can expand to the maximum capacity allocated to it.

4. Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

   Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

   Important: If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

5. Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. To deactivate Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Configure per disk**. **Note:** You can use the **Configure per disk** option to dowgrade from or upgrade to PMem storage. 2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

6. On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new storage location. Names of migrated virtual machine files on the destination datastore match the inventory name of the virtual machine.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource and Storage

You can move a virtual machine to another compute resource and move its disks or virtual machine folder to another datastore. With vMotion, you can migrate a virtual machine and its disks and files while the virtual machine is powered on.

- Required privilege: **Resource** > **Migrate powered on virtual machine**

Simultaneous migration to a new compute resource and datastore provides greater mobility for virtual machines by eliminating the vCenter Server boundary. Virtual machine disks or content of the virtual machine folder are transferred over the vMotion network to reach the destination host and datastores.

To make disk format changes and preserve them, you must select a different datastore for the virtual machine files and disks. You cannot preserve disk format changes if you select the same datastore on which the virtual machine currently resides.

1. Right-click the virtual machine and select **Migrate**.
   a) To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
   b) Click the **Virtual Machines** tab.
2. Select **Change both compute resource and storage** and click **Next**.
3. Select a destination resource for the virtual machine, and click **Next**.

   Any compatibility problems appear in the Compatibility panel. Fix the problem, or select another host or cluster.

   Possible targets include hosts and fully automated DRS clusters. If your target is a non-automated cluster, select a host within the non-automated cluster.

   If your environment has more than one vCenter Server instances, you can move virtual machines from one vCenter Server inventory to another.

   Important:

   If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

   If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks will use the storage policy and datastore selected for the configuration files of the virtual machine.

   Important: Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and choose a destination host that is licensed to use PMem devices.
4. On the Select storage page, select the storage type for the virtual machine configuration files and all the hard disks.
   - If you select the **Standard** mode, all virtual disks are stored on a standard datastore.
   - If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.
   - If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

5. Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation. Instead, it is zeroed out on demand on first write

Option	Action
	from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take

Option	Action
	longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can expand to the maximum capacity

Option	Action
	allocated to it.

6. Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

   Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

   Important: If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

7. Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same Storage DRS cluster.	1. Select a Storage DRS cluster. 2. To deactivate Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 3. Click **Next**.
Store virtual machine configuration files and disks in separate locations.	1. Click **Configure per disk**. **Note:** You can use the **Configure per disk** option to dowgrade from or upgrade to PMem storage individual hard disks. 2. For the virtual machine configuration file and for each virtual disk, select **Browse**, and select a datastore or Storage DRS cluster. **Note:** Configuration files cannot be stored on a PMem datastore. 3. If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the Storage DRS cluster. 4. Click **Next**.

8. Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

   You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

   You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

9. Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source

Option	Description
	and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants

Option	Description
	a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

10. On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Upgrading Virtual Machines

You can upgrade virtual machines to a higher level of compatibility and a higher version of VMware tools. After the upgrade, your VMs can take advantage of new hardware options and new features.

For a list of hardware features available to virtual machines with each ESXi hardware compatibility setting, see Hardware Features Available with Virtual Machine Compatibility Settings.

VMware Tools Upgrade

The first step in upgrading virtual machines is to upgrade VMware Tools. Installing VMware Tools is part of the process of creating a new virtual machine. If you are installing VMware Tools in multiple virtual machines with Windows guest operating systems, you can automate its installation and specify options for the components to include or exclude. For information about installing, upgrading, and configuring VMware Tools, see the *VMware Tools User Guide*.

If the virtual machines do not have VMware Tools installed, you can use the VMware Tools upgrade procedure to install VMware Tools. After you install or upgrade VMware Tools, upgrade the virtual machine compatibility.

Virtual Machine Compatibility Upgrade

VMware offers the following tools for upgrading virtual machines:

vSphere Client	Requires that you perform the virtual machine upgrade one step at a time, but does not require vSphere Lifecycle Manager. In the vSphere Client, you can upgrade virtual machines manually, or schedule upgrades.

	Manual Upgrade	Use this procedure to upgrade one or more virtual machines to the latest supported virtual hardware version immediately.
	Schedule VM Upgrades	Use this procedure to schedule an upgrade of one or more virtual machines at the next reboot of the virtual machine, and choose from all supported compatibility level upgrades.
vSphere Lifecycle Manager	Automates the process of upgrading and patching virtual machines, ensuring that the steps occur in the correct order. You can use vSphere Lifecycle Manager to directly upgrade virtual machine hardware, VMware Tools, and virtual appliances. You can also patch and update third-party software running on the virtual machines and virtual appliances. See the *vSphere Lifecycle Manager* documentation.	

Note: Do not use `vmware-vmupgrade.exe` to upgrade virtual machines.

Note: Upgrading virtual machine hardware is a heavyweight operation that might cause some applications or the operating system to stop working properly.

Downtime for Upgrading Virtual Machines

During a virtual machine compatibility upgrade, you must shut down the virtual machine for all guest operating systems. For VMware Tools upgrade, downtime is not required for many Linux operating systems.

Table 169: Virtual Machine Downtime by Guest Operating System

Guest Operating System	Upgrade VMware Tools	Upgrade Virtual Machine Compatibility
Microsoft Windows	Downtime to restart the guest operating system.	Downtime to shut down and power on the virtual machine.
Linux	Downtime to restart the guest operating system is required to load drivers.	Downtime to shut down and power on the virtual machine.
NetWare	No downtime.	Downtime to shut down and power on the virtual machine.
Solaris	No downtime.	Downtime to shut down and power on the virtual machine.
FreeBSD	No downtime.	Downtime to shut down and power on the virtual machine.
Mac OS X	No downtime.	Downtime to shut down and power on the virtual machine.

Note: For Linux guest operating systems, you must restart the virtual machine to load the new versions of the VMXNET, VMXNET3, and PVSCSI drivers. You can also manually reload the drivers. To verify that the drivers are configured in the Linux kernel and that the virtual hardware is available, see Knowledge Base article, http://kb.vmware.com/kb/2050364. Manual restart is not required for the Linux guest operating system using kernel version 3.10.

Planning Downtime for Virtual Machines

You can stagger virtual machine downtimes to accommodate a schedule convenient to you and your customers.

For example:

- If your virtual machine users are located in diverse time zones, you can prepare by migrating virtual machines to specific hosts to serve a given time zone. This way you can arrange host upgrades so that virtual machine downtime occurs transparently outside business hours for that time zone.
- If your virtual machine users operate around the clock, you can delay downtime for their virtual machines to normally scheduled maintenance periods. You do not need to upgrade any stage within a certain time period. You can take as long as needed at any stage.

Upgrade the Compatibility of a Virtual Machine Manually

The virtual machine compatibility determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host machine. You can upgrade the compatibility level to make additional hardware available to the virtual machine.

- Create a backup or snapshot of the virtual machines. See Using Snapshots To Manage Virtual Machines.
- Upgrade VMware Tools. On Microsoft Windows VMs, the virtual machine might lose its network settings if you upgrade the compatibility before you upgrade VMware Tools.
- Verify that all virtual machines and their `.vmdk` files are stored on storage connected to the ESXi host or the client machine.
- Determine the ESXi versions that you want the virtual machines to be compatible with. See Virtual Machine Compatibility.
- Check whether the guest operating systems of the virtual machines that you upgrade require a power off. For example, some Linux operating systems do not require a power-off before a virtual machine compatibility upgrade. See Virtual Machine Compatibility..

Important: Upgrading virtual machine hardware might cause some applications or the operating system to stop working properly. Perform a hardware version upgrade only if you need a feature that comes with the newer hardware version.

1. In the vSphere Client, navigate to the virtual machine.
2. Optional: Right-click the virtual machine and select **Power** > **Power Off**.
3. Select **Actions** > **Compatibility** > **Upgrade VM Compatibility**.
4. Click **Yes** to confirm the upgrade.
5. Select a compatibility and click **OK**.

Schedule a Compatibility Upgrade for a Virtual Machine

The virtual machine compatibility determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. You can schedule a compatibility upgrade to make a virtual machine compatible with newer versions of ESXi.

- Power off the virtual machine.
- Create a backup or snapshot of the virtual machine. See Using Snapshots To Manage Virtual Machines.
- Upgrade to the latest version of VMware Tools. If you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ ESXi host on a VMFS5 or NFS datastore.
- Verify that the virtual machine is stored on VMFS5 or NFS datastores.
- Verify that the compatibility settings for the virtual machine are not the latest supported version.

- Determine the ESXi version that you want the virtual machine to be compatible with. See Virtual Machine Compatibility.

Use this procedure to schedule an upgrade for one virtual machine at the next reboot of the virtual machine, and choose from all supported compatibility level upgrades. To upgrade virtual machines immediately to the latest supported compatibility, see Upgrade the Compatibility of a Virtual Machine Manually.

You can use this procedure to schedule an upgrade for multiple virtual machines.

For information about virtual machine hardware versions and compatibility, see Virtual Machine Compatibility.

1. Navigate to a virtual machine in the inventory.
2. Right-click the virtual machine and select **Compatibility** > **Schedule VM Compatibility Upgrade**.
3. In the **Schedule VM Compatibility Upgrade** dialog box, confirm that you want to schedule a compatibility upgrade by clicking **Yes**.
4. From the **Compatible with** drop-down menu, select the compatibility to upgrade to.

   The virtual machine compatibility is upgraded the next time you restart the virtual machine.
5. Optional: To upgrade the compatibility when you do regularly scheduled guest maintenance, select **Only upgrade after normal guest OS shutdown**.

   This prevents the scheduled upgrade from occurring unless the guest operating system of the virtual machine is shut down or restarted normally.

Each of the selected virtual machines is upgraded to the compatibility that you chose at the next reboot of the virtual machine, and the Compatibility setting is updated in the Summary tab of the virtual machine.

Required vCenter Server Privileges for Common Tasks

Many tasks require permissions on multiple objects in the vSphere inventory. If the user who attempts to perform the task only has privileges on one object, the task cannot complete successfully.

The following table lists common tasks that require more than one privilege. You can add permissions to inventory objects by pairing a user with one of the predefined roles or with multiple privileges. If you expect that you must assign a set of privileges multiple times, create custom roles. To learn more about required privileges for common tasks, see Privilege Recorder.

Refer to the *vSphere Web Services API Reference* documentation to learn how operations in the vSphere Client user interface map to API calls, and what privileges are required to perform operations. For example, the API documentation for the `AddHost_Task(addHost)` method specifies that the Host.Inventory.AddHostToCluster privilege is required to add a host to a cluster.

If the task that you want to perform is not in this table, the following rules explain where you must assign permissions to allow particular operations:

- Any operation that consumes storage space requires the **Datastore** > **Allocate Space** privilege on the target datastore, and the privilege to perform the operation itself. You must have these privileges, for example, when creating a virtual disk or taking a snapshot.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource** > **Assign Virtual Machine to Resource Pool** privilege.

Table 170: Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center: • **Virtual machine** > **Inventory** > **Create new** • **Virtual machine** > **Configuration** > **Add new disk** (if creating a new virtual disk) • **Virtual machine** > **Configuration** > **Add existing disk** (if using an existing virtual disk) • **Virtual machine** > **Configuration** > **Configure Raw device** (if using an RDM or SCSI pass-through device)	Administrator
	On the destination host, cluster, or resource pool: **Resource** > **Assign virtual machine to resource pool**	Resource pool administrator or Administrator
	On the destination datastore or the folder that contains the datastore: **Datastore** > **Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network** > **Assign network**	Network Consumer or Administrator
Power on a virtual machine	On the data center in which the virtual machine is deployed: **Virtual machine** > **Interaction** > **Power On**	Virtual Machine Power User or Administrator
	On the virtual machine or folder of virtual machines: **Virtual machine** > **Interaction** > **Power On**	
Deploy a virtual machine from a template	On the destination folder or data center: • **Virtual machine** > **Inventory** > **Create from existing** • **Virtual machine** > **Configuration** > **Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine** > **Provisioning** > **Deploy template**	Administrator
	On the destination host, cluster or resource pool: • **Resource** > **Assign virtual machine to resource pool** • **vApp** > **Import**	Administrator
	On the destination datastore or folder of datastores: **Datastore** > **Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network** > **Assign network**	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual machine** > **Snapshot management** > **Create snapshot**	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: • **Resource** > **Assign virtual machine to resource pool** • **Virtual machine** > **Inventory** > **Move**	Administrator
	On the destination resource pool: **Resource** > **Assign virtual machine to resource pool**	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: • **Virtual machine** > **Interaction** > **Answer question** • **Virtual machine** > **Interaction** > **Console interaction** • **Virtual machine** > **Interaction** > **Device connection** • **Virtual machine** > **Interaction** > **Power Off**	Virtual Machine Power User or Administrator

Task	Required Privileges	Applicable Role
	• **Virtual machine** > **Interaction** > **Power On** • **Virtual machine** > **Interaction** > **Reset** • **Virtual machine** > **Interaction** > **Configure CD media** (if installing from a CD) • **Virtual machine** > **Interaction** > **Configure floppy media** (if installing from a floppy disk) • **Virtual machine** > **Interaction** > **VMware Tools install**	
	On a datastore that contains the installation media ISO image: **Datastore** > **Browse datastore** (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image: • **Datastore** > **Browse datastore** • **Datastore** > **Low level file operations** • **Host** > **Configuration** > **System Management**	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: • **Resource** > **Migrate powered on virtual machine** • **Resource** > **Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource** > **Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: • **Resource** > **Migrate powered off virtual machine** • **Resource** > **Assign virtual machine to resource pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource** > **Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): **Datastore** > **Allocate space**	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource** > **Migrate powered on virtual machine**	Resource Pool Administrator or Administrator
	On the destination datastore: **Datastore** > **Allocate space**	Datastore Consumer or Administrator
On the destination cluster: • **Host** > **Inventory** > **Add host to cluster** • **Host** > **Inventory** > **Modify cluster**	Administrator	
Add a single host to a data center by using the vSphere Client, or add a single host to a cluster by using PowerCLI or API (leveraging the addHost API)	On the host: **Host** > **Inventory** > **Add host to cluster**	Administrator
	On the cluster: • **Host** > **Inventory** > **Modify cluster** • **Host** > **Inventory** > **Add host to cluster**	Administrator
	On the data center: **Host** > **Inventory** > **Add standalone host**	Administrator
Add multiple hosts to a cluster	On the cluster:	Administrator

Task	Required Privileges	Applicable Role
	• **Host** > **Inventory** > **Modify cluster** • **Host** > **Inventory** > **Add host to cluster**	
	On the parent data center of the cluster (with propagate): • **Host** > **Inventory** > **Add standalone host** • **Host** > **Inventory** > **Move host** • **Host** > **Inventory** > **Modify cluster** • **Host** > **Configuration** > **Maintenance**	Administrator
Encrypt a virtual machine		Administrator
Protect a virtual machine (if using vSphere+ to protect the virtual machine)	On the data center in which the virtual machine is deployed: • **vSphere Tagging** > **Assign or Unassign vSphere Tag**	Administrator

Troubleshooting Overview

vSphere Troubleshooting contains common troubleshooting scenarios and provides solutions for each of these problems. You can also find guidance here for resolving problems that have similar origins. For unique problems, consider developing and adopting a troubleshooting methodology.

The following approach for effective troubleshooting elaborates on how to gather troubleshooting information, such as identifying symptoms and defining the problem space. Troubleshooting with log files is also discussed.

Guidelines for Troubleshooting

To troubleshoot your implementation of vSphere, identify the symptoms of the problem, determine which of the components are affected, and test possible solutions.

Identifying Symptoms
A number of potential causes might lead to the under-performance or nonperformance of your implementation. The first step in efficient troubleshooting is to identify exactly what is going wrong.

Defining the Problem Space
After you have isolated the symptoms of the problem, you must define the problem space. Identify the software or hardware components that are affected and might be causing the problem and those components that are not involved.

Testing Possible Solutions
When you know what the symptoms of the problem are and which components are involved, test the solutions systematically until the problem is resolved.

Identifying Symptoms

Before you attempt to resolve a problem in your implementation, you must identify precisely how it is failing.

The first step in the troubleshooting process is to gather information that defines the specific symptoms of what is happening. You might ask these questions when gathering this information:

- What is the task or expected behavior that is not occurring?
- Can the affected task be divided into subtasks that you can evaluate separately?
- Is the task ending in an error? Is an error message associated with it?
- Is the task completing but in an unacceptably long time?
- Is the failure consistent or sporadic?
- What has changed recently in the software or hardware that might be related to the failure?

Defining the Problem Space

After you identify the symptoms of the problem, determine which components in your setup are affected, which components might be causing the problem, and which components are not involved.

To define the problem space in an implementation of vSphere, be aware of the components present. In addition to VMware software, consider third-party software in use and which hardware is being used with the VMware virtual hardware.

Recognizing the characteristics of the software and hardware elements and how they can impact the problem, you can explore general problems that might be causing the symptoms.

- Misconfiguration of software settings
- Failure of physical hardware
- Incompatibility of components

Break down the process and consider each piece and the likelihood of its involvement separately. For example, a case that is related to a virtual disk on local storage is probably unrelated to third-party router configuration. However, a local disk controller setting might be contributing to the problem. If a component is unrelated to the specific symptoms, you can probably eliminate it as a candidate for solution testing.

Think about what changed in the configuration recently before the problems started. Look for what is common in the problem. If several problems started at the same time, you can probably trace all the problems to the same cause.

Testing Possible Solutions

After you know the problem's symptoms and which software or hardware components are most likely involved, you can systematically test solutions until you resolve the problem.

With the information that you have gained about the symptoms and affected components, you can design tests for pinpointing and resolving the problem. These tips might make this process more effective.

- Generate ideas for as many potential solutions as you can.
- Verify that each solution determines unequivocally whether the problem is fixed. Test each potential solution but move on promptly if the fix does not resolve the problem.
- Develop and pursue a hierarchy of potential solutions based on likelihood. Systematically eliminate each potential problem from the most likely to the least likely until the symptoms disappear.
- When testing potential solutions, change only one thing at a time. If your setup works after many things are changed at once, you might not be able to discern which of those things made a difference.
- If the changes that you made for a solution do not help resolve the problem, return the implementation to its previous status. If you do not return the implementation to its previous status, new errors might be introduced.
- Find a similar implementation that is working and test it in parallel with the implementation that is not working properly. Make changes on both systems at the same time until few differences or only one difference remains between them.

Troubleshooting with vCenter Server Logs

You can often obtain valuable troubleshooting information by looking at the logs provided by the various services and agents that your implementation is using.

Most logs are located in `/var/log/vmware/<service_name>` for vCenter Server deployments.

Common Logs

The following logs are common to all vCenter Server deployments.

Table 171: Common Log Directories

Log Directory	Description
`../firstboot`	Stores first boot logs
`applmgmt` and `applmgmt-audit`	Stores logs related to the VMware Appliance Management Service
`cloudvm`	Stores logs for allotment and distribution of resources between services
`rhttpproxy`	Stores logs for the VMware HTTP Reverse Proxy service
`sca`	Stores logs for the VMware Service Control Agent service
`vapi`	Stores logs for the VMware vAPI Endpoint service
`vmafdd`	Stores logs for the VMware Authentication Framework - LDAP service
`vmdird`	Stores logs for the VMware Directory Service - LDAP service
`vmon`	Stores logs for the VMware Service Lifecycle Manager service

Management Node Logs

The following logs are available if a management node deployment is selected.

Table 172: Management Node Log Directories

Log Directory	Service
`rbd`	VMware vSphere Auto Deploy
`content-library`	VMware Content Library Service
`eam`	VMware ESX Agent Manager
`netdumper`	VMware vSphere ESXi Dump Collector
`perfcharts`	VMware Performance Charts Service
`vmcam`	VMware vSphere Authentication Proxy
`vmdird`	VMware Directory Service - LDAP
`vmware-sps`	VMware vSphere Profile-Driven Storage Service
`vpxd`	VMware vCenter Server
`vpostgres`	VMware Postgres service
`vcha`	VMware vCenter High Availability service

Troubleshooting Virtual Machines

The virtual machine troubleshooting topics provide solutions to potential problems that you might encounter when using your virtual machines.

Troubleshooting USB Passthrough Devices

Information about feature behavior can help you troubleshoot or avoid potential problems when USB devices are connected to a virtual machine.

Error Message When You Try to Migrate Virtual Machine with USB Devices Attached

Migration with vMotion cannot proceed and issues a confusing error message when you connect multiple USB devices from an ESXi host to a virtual machine and one or more devices are not enabled for vMotion.

The Migrate Virtual Machine wizard runs a compatibility check before a migration operation begins. If unsupported USB devices are detected, the compatibility check fails and an error message similar to the following appears: `Currently connected device 'USB 1' uses backing 'path:1/7/1', which is not accessible.`

To successfully pass vMotion compatibility checks, you must enable all USB devices that are connected to the virtual machine from a host for vMotion. If one or more devices are not enabled for vMotion, migration will fail.

1. Make sure that the devices are not in the process of transferring data before removing them.
2. Re-add and enable vMotion for each affected USB device.

Cannot Copy Data From an ESXi Host to a USB Device That Is Connected to the Host

You can connect a USB device to an ESXi host and copy data to the device from the host. For example, you might want to gather the vm-support bundle from the host after the host loses network connectivity. To perform this task, you must stop the USB arbitrator.

If the USB arbitrator is being used for USB passthrough from an ESXi host to a virtual machine the USB device appears under `lsusb` but does not mount correctly.

This problem occurs because the nonbootable USB device is reserved for the virtual machine by default. It does not appear on the host's file system, even though `lsusb` can see the device.

1. Stop the `usbarbitrator` service:`/etc/init.d/usbarbitrator stop`
2. Physically disconnect and reconnect the USB device.
   By default, the device location is `/vmfs/devices/disks/mpx.vmhbaXX:C0:T0:L0`.
3. After you reconnect the device, restart the `usbarbitrator` service:`/etc/init.d/usbarbitrator start`
4. Restart `hostd` and any running virtual machines to restore access to the passthrough devices in the virtual machine.

Recover Orphaned Virtual Machines

Virtual machines appear with `(orphaned)` appended to their names.

Virtual machines that reside on an ESXi host that vCenter Server manages might become orphaned in rare cases. Such virtual machines exist in the vCenter Server database, but the ESXi host no longer recognizes them.

Virtual machines can become orphaned if a host failover is unsuccessful, or when the virtual machine is unregistered directly on the host. If this situation occurs, move the orphaned virtual machine to another host in the data center on which the virtual machine files are stored.

1. Determine the datastore where the virtual machine configuration (`.vmx`) file is located.
   a) Select the virtual machine in the inventory, and click the **Datastores** tab.
      The datastore or datastores where the virtual machine files are stored are displayed.

b) If more than one datastore is displayed, select each datastore and click the **Files** tab to browse for the `.vmx` file.
c) To verify the location of the `.vmx` file, select the virtual machine from **Datastore**.

2. Return to the virtual machine in the inventory, right-click it, and select **Remove from Inventory**.
3. Click **Yes** to confirm the removal of the virtual machine.
4. Reregister the virtual machine with vCenter Server.
   a) Right-click the datastore where the virtual machine file is located and select **Register VM**.
   b) Browse to the `.vmx` file and click **OK**.
   c) Select the location for the virtual machine and click **Next**.
   d) Select the host on which to run the virtual machine and click **Next**.
   e) Click **Finish**.

vSphere Host Profiles

Learn how to manage and configure Host Profiles in the vSphere Client.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

The *vSphere Host Profiles* documentation is intended for administrators who are familiar with vSphere host configuration.

Updated Information

This *vSphere Host Profiles* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Host Profiles* documentation.

Revision	Description
05 JAN 2024	Added more information about importing host customizations in Edit Host Customizations.
12 SEP 2023	Updated the procedure in Edit a Host Profile.
05 OCT 2021	Initial release.

Introduction To vSphere Host Profiles

The Host Profiles feature creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages multiple hosts or clusters in vCenter Server.

Host Profiles provide an automated and centrally managed mechanism for host configuration and configuration compliance. Host Profiles can improve efficiency by reducing reliance upon repetitive, manual tasks. Host Profiles capture the configuration of a pre-configured and validated reference host, store the configuration as a managed object and use the catalog of parameters contained within to configure networking, storage, security, and other host-level parameters. Host Profiles can be applied to individual hosts, a cluster, or all the hosts and clusters associated to a host profile. Applying a Host Profile to a cluster affects all hosts in the cluster and result in a consistent configuration across the applied hosts.

Host Profiles can be used to validate the configuration of a host by checking compliance of a host or cluster against the Host Profile that is associated with that host or cluster.

Host Profiles Usage Model

The Host Profiles workflow starts with the concept of a reference host. The configuration of the reference host, which is extracted as a host profile, serves as a configuration template for configuring other hosts. The reference host does not have to be related or associated with the host profile extracted from it.

Before you begin, ensure that you have an existing vSphere environment installation with at least one properly configured ESXi host.

The sequence required to create a host profile from a reference host, apply the host profile to a host or cluster and check compliance against the host profile is as follows:

1. Set up and configure the reference host.
2. Create a host profile from the reference host.

3. Attach hosts or clusters to the host profile.
4. Check the compliance to the host profile. If all hosts are compliant with the reference host, they are correctly configured.
5. Apply (remediate).

As a licensed feature of vSphere, Host Profiles are only available when the appropriate licensing is in place. If you see errors, ensure that you have the appropriate vSphere licensing for your hosts.

If you want the Host Profile to use directory services for authentication, the reference host needs to be configured to use a directory service. See the *vSphere Security* documentation.

vSphere Auto Deploy

For hosts provisioned with vSphere Auto Deploy, vSphere Client owns the entire host configuration, which is captured in a Host Profile. Usually, the Host Profile information is sufficient to store all configuration information. Sometimes the user is prompted for input when the host provisioned with Auto Deploy starts. See the *VMware ESXi Installation and Setup* documentation for more information on Auto Deploy.

Reference Host Independence

A dedicated reference host is not required to be available to perform host profile tasks.

When you create a host profile, you extract the configuration information from a specified ESXi reference host. In previous releases, vSphere required that the reference host was available for certain Host Profiles tasks, such as editing, importing, and exporting. From vSphere 6.0 and later, a dedicated reference host is no longer required to be available to perform these tasks. For host profile tasks that require a reference host, an ESXi host that is compatible to the host profile is assigned as a reference host.

Sometimes, a compatible host is not available to validate the host profile during these tasks. If you make small changes to the host profile, validation is skipped and a you see a warning indicating that no valid reference host is associated with the profile. You can then proceed and finish the task.

Due to the introduction of this feature, users can no longer edit or change the reference host from the vSphere Client. The reference host selection occurs at runtime, without notifying users, in the vCenter Server for on-going tasks.

Reference Host Selection

To select a suitable reference host, vCenter Server performs complex version and compatibility checks on the target host.

Starting with vSphere 7.0 Update 3, a major-version vCenter Server instance can manage hosts of all ESXi Update release versions within the respective major version. For example, a vCenter Server 7.0 Update 3 instance can manage ESXi hosts and hosts profiles of version 7.0 GA, 7.0 Update 1, 7.0 Update 2, and 7.0 Update 3. This change affects the reference host selection for particular host profile operations.

Version Check

To select a reference host, vCenter Server checks whether the target host is of the same ESXi Update release version as the host profile. For some operations, the target host can run a later ESXi version than the ESXi version of the host profile. For example, if you want to edit a 7.0 Update 3 host profile, the reference host that validates the host profile cannot be running ESXi 7.0 GA, 7.0 Update 1, or 7.0 Update 2.

Compatibility Check

In addition to checking the version on the target host, vCenter Server performs an extensive compatibility check that includes a subprofile compatibility check in the existing releases. Starting with vSphere 7.0 Update 3, to appoint a reference host, vCenter Server checks the advanced options and the default roles in the target host. A reference host

must support the advanced options of the host profile it validates. Also, the default roles in the reference host must match the default roles in the host profile.

Host Profile Operations and Required Reference Host Versions

A reference host is needed to validate the host profile during different host profile operations and workflows. Starting with vSphere 7.0 Update 3, depending on the operation, the reference host must be of exactly the same or later Update release version as the host profile it validates. The following table summarizes the compatible reference host versions for different host profile operations if your environment runs a vCenter Server instance 7.0 Update 3 or later.

Host Profile Operation	Compatible Reference Host Version
Edit	The same Update release version as the host profile.
Check Compliance	The same or later Update release version as the host profile.
Remediation	The same or later Update release version as the host profile.
Attach	The same or later version as the host profile.
Import/Export	The exact same version as the host profile.

Note: If the vCenter Server instance is of version earlier than 7.0 Update 3, Update release versions are not checked during the selection of a reference host. vCenter Server only checks if the reference host and the host profile are of the same major release version, for example 6.x or 7.x.

Using Host Profiles

This section describes how to perform some of the basic tasks for Host Profiles.

Access Host Profiles

The Host Profiles main view lists all available profiles. Administrators can also use the Host Profiles main view to perform operations on host profiles and configure them.

1. In the vSphere Client, from the main menu, select **Policies and Profiles**.
2. Select **Host Profiles**.

Create a Host Profile

You create a host profile by extracting the configuration from a designated reference host.

Verify that you have a working vSphere installation and at least one completely and properly configured host.

Note: Host profiles do not capture offline or non-present devices. Any changes made to offline devices after extracting a host profile do not make a difference to the compliance check results.

1. Navigate to the **Host Profiles** main view and click **Extract Host Profile**.
2. On the **Select host** page, select the vCenter Server instance where to create the host profile.
3. Select the host that acts as the reference host and click **Next**.
   The selected host must be a valid host.
4. Enter a name and, optionally, a description for the new profile, and click **Finish**.

The new profile appears in the **Host Profiles** pane.

Attach or Detach Hosts and Clusters to a Host Profile

After creating a host profile from a reference host, you must attach a host or cluster to the host profile to associate that host profile with the selected host or cluster. To disassociate a configuration from an ESXi host or an entire cluster, that host or cluster must be detached from the host profile.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the entire cluster, there is no association between the host or hosts within the cluster and that host profile. Detaching a host profile from an ESXi host or a cluster does not delete that host profile. You can delete the host profile after detaching it from all the entities it is associated with.

Note: You can also attach or detach a host profile by right-clicking the specific host and select **Host Profiles** > **Attach Host Profile** or **Host Profiles** > **Detach Host Profile**. This process is non-disruptive.

1. Navigate to **Host Profiles** main view.
2. Right-click the host profile and select **Attach/Detach Hosts and Clusters** .
3. Select or deselect the hosts or clusters from the list and click **Save**.
   You can use the **Filter** text box to search the hosts and clusters list.

The hosts or clusters are added or removed from the selected host profile.

Check Compliance

You can confirm the compliance of a host or cluster to its attached host profile and determine which, if any, configuration parameters on a host are different from those specified in the host profile.

1. Navigate to **Host Profiles** main view.
2. Right click a host profile.
3. Click **Check Host Profile Compliance**.

The compliance status is updated as Compliant, Unknown, or Non-compliant.

A non-compliant status indicates a discovered and specific inconsistency between the profile and the host. To resolve this, you should remediate the host. Any unknown status indicates that the compliance of the host cannot be verified; to resolve the issue, remediate the host through the host profile. Often the compliance check fails because the host is disconnected.

Note: Host profiles do not capture offline or unpresented devices. Any changes made to offline devices after extracting a host profile do not make a difference to the compliance check results.

To see more detail on compliance failures, select a host profile from the **Host Profiles** main view for which the last compliance check produced one or more failures. To see specific detail on which parameters differ between the host that failed compliance and the host profile, click the **Monitor** tab and select the Compliance view. Then select the failing host. The differing parameters are displayed in the Compliance window, below the host list.

Schedule Compliance Check

You can schedule a regular compliance check of a host or cluster, using a standard vSphere Client scheduled tasks workflow. This automation determines, if any configuration parameters are different from those specified in the host profile.

1. Navigate to **Host Profiles** main view.
2. Select the desired host profile and navigate to the **Monitor** tab.
3. From the **Monitor** tab, select **Scheduled Tasks** -> **New Scheduled Task** -> **Check Compliance**.
   The **Schedule New Tasks (Check Compliance)** dialog box appears.

4. Optional: Enter a new task name.
   Additional details about the task can be entered in the **Description** text box.
5. Choose a frequency how often to run the task.
   You can postpone when the task is run for the first time and schedule when it ends.
6. Optional: To receive a notification after the task is finished, enter an email.
7. Click **Schedule The Task**.

The newly created task is visible on the **Scheduled Tasks** list.

Note: You can **Edit**, **Run** or **Remove** the task.

To understand more about compliance status, checks or failures, see **Check Compliance**.

Remediate a Host

If there is a compliance failure, use the remediate option to apply the host profile settings to the host. This action changes all host profile parameters to the values defined in the host profile that is attached to the host.

Verify that a host profile is attached to the host.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Right-click the host profile and select **Remediate**.

   Note: Certain Host Profile policy configurations require that the host is rebooted after remediation. In such cases, you are prompted to place the host into maintenance mode. You might be required to place hosts into maintenance mode before remediation. Hosts that are in a fully automated DRS cluster are placed into maintenance mode during remediation. Alternatively, if the host is not placed into maintenance mode when required, the remediation process stops.
3. Select the hosts you want to remediate against the host profile.
   The host profile is applied to each host that you select.
4. Optional: To specify host properties, enter your host customizations or import a host customization file.

   You can modify the user input parameters for the host profiles policies by customizing the host and clicking **Next**.

   Note: See Host Profiles and vSphere Auto Deploy for more information about vSphere Auto Deploy.
5. To check if the selected hosts can be remediated, click **Pre-check Remediation**.
   The pre-check generates a list of tasks that will be performed on the host.
6. If needed, select the check box to reboot the hosts.
   Alternatively you can reboot the hosts manually after the remediation process.
7. Review the tasks that are necessary to remediate the host profile and click **Finish**.

The compliance status is updated.

Edit a Host Profile

You can view and edit Host Profiles policies, select a policy to be checked for compliance, and change the policy name or description.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Under **Policies and Profiles**, click **Host Profiles**.
3. Right-click the host profile that you want to edit and click **Edit Host Profile**.
4. Optional: Click the Name and description tab to change the profile name and description.
5. In the **Settings** tab, expand each category to view or edit particular policies or settings.

   Note: See Edit a Policy for detailed instructions for editing a Host Profile policy. See Disable Host Profile Component or Subprofile for detailed instructions on enabling or disabling a policy from compliance check or remediation.
6. View **All** host profile configurations or only **Favorites** configurations.

   You can mark a configuration as a favorite with the star icon. Those are then added to **Favorites** configurations.
7. Optional: In the search field, filter the configuration names and values you want to view.
   For example, enter `SNMP`. All configurations that relate to **SNMP** are displayed.
8. Optional: Customize the hosts.

   Make any changes to the available configuration values for this profile and click **Save**.

   Note: The host customization settings page only appears if you changed any settings that require host customizations.

The changes are made when the "Update Host Profile" task is completed in the Recent Tasks status. If you attempt to remediate the profile before the task is complete, the profile configuration does not contain the change.

Edit a Policy

A policy describes how a specific configuration setting is applied. You can edit policies belonging to a specific Host Profile.

When you edit the Host Profile, you can expand the Host Profile's configuration hierarchy to see the sub-profile components that comprise the Host Profile. These components are categorized by functional group or resource class to make it easier to find a particular parameter. Each subprofile component contains one or more attributes and parameters, with the policies and compliance checks.

Each policy consists of one or more options that contain one or more parameters. Each parameter consists of a key and a value. The value can be one of a few basic types, for example integer, string, string array, or integer array.

Note: Currently, there is no way to remove or replace policy options policies, or sub-profiles that are deprecated in this release. Metadata is added to these deprecated policies that allows old host profiles to continue working but will extract new host profiles with only non-deprecated parts of a host profile.

Table 173: Subset of Host Profile Subprofile Configurations

Component Categories	Configuration Settings	Notes and Examples
Advanced Configuration Settings	Advanced Options, Agent VM, DirectPath I/O, Hosts file, Power System, System Image Cache	• Host Profiles do not check advanced settings if they are the same as the default settings. vCenter Server copies only the advanced configuration settings that have changed and that differ from the default values. In addition, compliance checks are limited to the settings that are copied.

Component Categories	Configuration Settings	Notes and Examples
		• Host Profiles does not support the configuration of PCI devices for virtual machine passthrough on the ESXi host.
General System Settings	Console, Core Dump, Device Alias, Host Cache, Kernel Module, Management Agent, System Resource Pool, System Swap, vFlash Host Swap Cache, CIM-XML Indication Subscriptions	For Date and Time Configuration: • For the time zone, enter a UTC string. For example, "America/Los_Angeles" for United States Pacific time zone. • The default time zone is set to the local time and location of the vSphere Client machine. • Configure Network Time Protocol (NTP) correctly. You can configure the NTP settings on the host's **Configure** tab. Click **Time Configuration** (under System). Click **Edit** to configure the time settings . **Note:** Enter host cache size as a whole GB in MB. For example, 1024 MB.
Networking	vSwitch, Port groups, Physical NIC speed, security and NIC teaming policies, vSphere Distributed Switch, and vSphere Distributed Switch uplink port.	When DHCPv6 is enabled in the networking subprofile, manually turn on the corresponding rule set in the firewall subprofile.
Security	Firewall, Security Settings, Service	
Storage	Configure storage options, including Native Multi-Pathing (NMP), Pluggable Storage Architecture (PSA), FCoE and iSCSI adapters, and NFS storage.	• Use the vSphere CLI to configure or modify the NMP and PSA policies on a reference host, and then extract the Host Profile from that host. If you use the Profile Editor to edit the policies, to avoid compliance failures, make sure that you understand interrelationships between the NMP and PSA policies and the consequences of changing individual policies. For information about the NMP and PSA, see the *vSphere Storage* documentation. • Add the rules that change device attributes before extracting the Host Profile from the reference host. After attaching a host to the Host Profile, if you edit the profile and change the device attributes (for example, mask device paths or adding SATP rules to mark the device as SSD) you are prompted to reboot the host to make the changes. However, after rebooting, compliance failures occur because the attributes changed. Because Host Profiles extract device attributes before rebooting, if any changes occur after the reboot, it evaluates and finds those changes, and reports it as noncompliant.

Component Categories	Configuration Settings	Notes and Examples
		• Use the vSphere Client to configure or modify the SatpDeviceProfile policy after extracting the Host Profile. For compliance purposes, the policy option strings must be in the following format: – For an ALUA supported array, for example, SATP_ALUA, the policy options must be separated by a semicolon (;). For example: `implicit_support=<on/off>; explicit_support=<on/off>; action_onRetryErrors=<on/off>` – For an ALUA supported array with CX, for example, SATP_ALUA_CX, the policy options must be separated by a semicolon (;). For example: `navireg=<on/off>; implicit_support=<on/off>; action_onRetryErrors=<on/off>` – For a CX array, for example, SATP_CX or SATP_INV, the policy options must be separated by a space. For example: `navireg=<on/off> ipfilter=<on/off> action_onRetryErrors=<on/off>` **Note:** The policy configuration options that are marked with `off` are not present in the configuration string.

Other profile configuration categories include: user group, authentication, kernel module, DCUI keyboard, host cache settings, SFCB, resource pools, login banner, SNMP agent, power system, and CIM indication subscriptions.

1. Edit the Host Profile.
2. Expand a subprofile until you reach the policy to edit.
3. Select the policy.
   The policy options and parameters appear on the right side of the **Edit Host Profile** dialog box.
4. Make changes to the policy.

Disable Host Profile Component or Subprofile

You can decide whether a host profile component or subprofile is applied or considered during a compliance check. This action allows administrators to eliminate non-critical attributes from consideration or ignore values that, while part of the host profile, are likely to vary between hosts.

1. Edit a host profile.
2. Expand the Host Profile Component hierarchy until you reach the desired component or component element.
3. Disable the check box next to a component.
   The check box is enabled by default. If you disable the check box, the other subprofiles that are enabled are still applied and selected.

The component or component element is not considered during a profile compliance check or applied during remediation. **Note:** Sometimes, disabling the check box might remove the component or component element from the host. This action is displayed in the task list after the pre-check remediation.

Duplicate a Host Profile

A host profile duplicate is a copy of an existing host profile.

1. Navigate to the **Host Profiles** main view and select the host profile you want to duplicate.
2. Click **Duplicate Host Profile**.
3. Type different name and description for the duplicate Host Profile, and click **OK**.

A clone of the profile appears in the Host Profiles list.

Copy Settings from Host

If the configuration of the reference host changes, you can update the host profile so that it matches the reference host's new configuration.

After you create a host profile, you can make incremental updates to the profile. When making changes to a host profile, consider the benefits and limitations of the two methods:

- Make the configuration changes to a host and copy that host's settings to the profile. The settings within the existing profile are updated to match those of the host. This method allows you to validate the configuration on a single host before rolling it to the other hosts that are attached to the profile.
- Update the profile directly by editing the host profile. This provides the ability to do more comprehensive and immediate remediation of those changes.

Note: Fixed user password, system image cache and some of the host customized settings are not present in the newly updated host profile. Edit the host profile to update these settings.

1. Navigate to the **Host Profiles** main view and select the host profile.
2. Click **Copy Settings from Host**.
3. Select the host from which you want to copy the configuration settings.
4. Click **OK**.

Host Profiles and vSphere Auto Deploy

You can use Host Profiles and vSphere Auto Deploy to provision physical ESXi hosts with a complete and expected configuration state for virtual switches, driver settings, boot parameters, and so on.

Because hosts that are provisioned with Auto Deploy are considered to be stateless, configuration state information is not stored on the host. Instead, you create and configure a reference host. Then, you create a host profile from the reference host. Next, you associate the host profile with an Auto Deploy rule. As a result new hosts that you provision with Auto Deploy have the host profile applied automatically.

Remediation for these hosts is the same as statefully deployed hosts. When you apply the host profile, you are prompted to customize the hosts and enter answers for the policies that you specified during the host profile creation.

Note: If you deploy ESXi with Auto Deploy, configure a `syslog` to store logs in a remote server. For more information on setting up a syslog from the Host Profiles interface, see the *vSphere Installation and Setup* documentation.

For more information on setting up an Auto Deploy reference host, see the *VMware ESXi Installation and Setup* documentation.

Import a Host Profile

You can import a profile from a file in the VMware profile format (`.vpf`).

When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Click **Import Host Profile**.
3. Click **Browse** to locate the VMware Profile Format file (`.vpf`) to import.
4. Enter the **Name** and **Description** for the imported Host Profile, and click **OK**.

The imported profile appears in the profile list.

Export a Host Profile

You can export a profile to a file that is in the VMware profile format (`.vpf`).

When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in a plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Right-click the profile and select **Export Host Profile**.
3. Click **Save**.

Copy Settings to Host Profile

After you make changes to a host profile, you can propagate those changes to other host profiles in the inventory.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Right-click the profile and select **Copy Settings to Host Profiles**.
3. Select the settings you want to copy to other host profiles, and click **Next**.
4. Select the target host profile that will be overwritten with the selected settings, and click **Next**.
   The differences between the host profile settings are displayed on the **Ready to complete** page.
5. Click **Finish**.

Configuring Host Profiles

This section describes how to configure host profiles using the host profile editor.

Host Customization

To customize hosts with shared attributes, you can create a host profile in a reference host. To customize individual hosts, you can set up some fields in the host profile to prompt the user for input for each host.

Host profiles allow you to prespecify information, for example, the storage setup or Syslog setup in a reference host to and apply the host profile to a set of target hosts that share the same settings. You can also use host profiles to specify that certain settings are host dependent. If you do so, the host comes up in maintenance mode when you provision it with Auto Deploy. Remediate the host or reset the host customization to be prompted for input. The system stores your input and uses it the next time the host boots.

When the host profile is set to prompt for user input, you must specify a value in the dialog that appears when you reset the host customization. An error results if you do not specify a value.

Table 174: Host Profile Options that Prompt for iSCSI User Input

Information to Request User Input For		Setting the Host Profile Option
When you apply a host profile on a system that includes a profile for iSCSI, you are prompted for several properties. For many of the properties, a system default is available. For some properties, you must specify a value or an error results.		1. Select **Edit Host Profile**, click **Storage configuration**, and click **iSCSI Initiator Configuration**. 2. Select the folder for an already enabled initiator and set up the initiator. 3. Set up the initiator. For many fields, the user is prompted as part of host customization.
IQN name	If the iSCSI setup uses an IQN name, you are prompted when you apply the host profile. You cannot continue until you provide the name.	
CHAP information	If you set up iSCSI to require CHAP authentication, you are prompted for CHAP information including the user name and the secret when you apply the host profile. You cannot continue until you provide the name.	

Table 175: Host Profile Options that Prompt for Storage User Input

Information to Request User Input For	Setting the Host Profile Option
You are setting up the Fixed PSP configuration and want to prompt for the adapter and target IDs for the storage arrays that should use the Fixed PSP.	You can set the option only if the adapter is set up to use the Fixed PSP. 1. Select **Edit Host Profile**, click **Storage configuration**. 2. Click **Native Multipathing (NMP)**. 3. Click **Path Selection Policy (PSP) configuration**. 4. In the Preferred Path window, select **Prompt the user for adapter and target IDs on the host**.
Configure FCoE adapter activation based on a user-specified MAC address.	You can set the option only if an activation profile exists. 1. Select **Edit Host Profile**, click **Storage configuration**. 2. Click **Software FCoE configuration**. 3. Click **Adapter Configuration**. 4. Click the activation profile and click **Policy Profile**. 5. Select **Activation policy based on adapter MAC address** from the drop-down menu.

Table 176: Host Profile Options that Prompt for Security User Input

Information to Request User Input For	Setting the Host Profile Option
Administrator password for ESXi host when the host boots for the first time.	1. Select **Edit Host Profile**, and click **Security and Services**. 2. click **Security Settings** and click **Security configuration**. 3. In the right panel, select **User Input Password to be Used to Configure Administrator Password** from the **Administrator password** drop-down menu.

Information to Request User Input For	Setting the Host Profile Option
Preconfigures a user for the ESXi host but prompts for the password for that user on each host when the host boots for the first time.	You can perform this task only if a user configuration already exists. Configure the user by selecting one of the options. • **Assigned fixed user configurations** is available for compatibility with ESX/ESXi 4.1 system, this option displays the password in the clear. • **Assign advanced fixed user configurations** is for users of ESXi 5.0 and later systems. • **Specify the user configuration in the profile but prompt for password during host configuration** allows you to specify the information about the user but prompt for a password on each host.
Prompt the user for credentials when the host joins the Active Directory domain.	1. Set the Authentication configuration profile to use a fixed domain. a. Select **Edit Host Profile**, click **Security and Services**. b. Click **Security Settings**, and click **Authentication configuration**. c. Click **Active Directory configuration**. d. In the Domain Name drop-down menu, select **Configure a fixed domain name**. 2. Set the method for joining the domain to prompt the user. a. Select **Edit Host Profile**, click **Security and Services** and click **Authentication configuration**. b. Click **Active Directory configuration**. c. In the Join Domain Method drop-down menu, select **Use user specified AD credentials to join the host to domain**.

Table 177: Host Profile Options that Prompt for Networking User Input

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the MAC address for a port group. You can have the system prompt the user in all cases (User specified MAC address...) or prompt the user only if no default is available.	1. Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2. Click **Management Network**. 3. In the **Determine how MAC address for vmknic should be decided** field, select how the system manages the MAC address. — **User specified MAC Address to be used while applying the configuration** — **Prompt the user for the MAC Address if no default is available**
Prompt the user for the IPv4 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv4 address...) or prompt the user only if no default is available.	1. Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2. Click **Management Network** and click **IP address settings**. 3. In the **IPv4 address** field, select how the system manages the IPv4 address. — **User specified IPv4 Address to be used while applying the configuration** — **Prompt the user for the IPv4 Address if no default is available**

Information to Request User Input For	Setting the Host Profile Option
Prompt the user for the IPv6 address for each ESXi host to which the profile is applied. You can have the system prompt the user in all cases (User specified IPv6 address...) or prompt the user only if no default is available.	1. Select **Edit Host Profile,** click **Networking configuration**, and click **Host port group**. 2. Click **Management Network** and click **IP address settings**. 3. In the **Static IPv6 address** field, select how the system manages the IPv6 address. — **User specified IPv6 Address to be used while applying the configuration** — **Prompt the user for the IPv6 Address if no default is available**
Prompt the user for the DNS name of the host. You can have the system prompt the user in all cases (User specified host name...) or prompt the user only if no default is available.	1. Select **Edit Host Profile,** click **Networking configuration**, and click **DNS configuration**. 2. In the Host name field, select how the system manages the DNS configuration. — **Prompt the user for host name if default is not available** — **User specified host name to be used while applying the configuration**
Prompt the user for the MAC address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user in all cases or only if no default is available.	1. Open **Networking configuration**. 2. Click **Host virtual NIC**. 3. In the **Determine how MAC address for vmknic should be decided** field, select how the system manages the MAC address for the distributed switch. — **User specified MAC address to be used while applying the configuration** — **Prompt the user for the MAC address if no default is available**
Prompt the user for the IPv4 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1. Open **Networking configuration**. 2. Click **Host virtual NIC**. 3. Click **IP address settings**. 4. In the IPv4 address field, select how the system handles the IPv4 address for the distributed switch. — **User specified IPv4 address to be used while applying the configuration** — **Prompt the user for IPv4 address if no default is available**
Prompt the user for the IPv6 address for a distributed switch, its port group, or one of its services. Right-click the Host virtual NIC folder icon and click the **Add sub-profile** icon to determine the component to which the setting is applied. You can decide to prompt the user only if no default is available or in all cases.	1. Open **Networking configuration**. 2. Open **Host virtual NIC**. 3. Open **IP address settings**. 4. In the **Static IPv6 address** field, select how the system manages the IPv6 address for the distributed switch. — **User specified IPv6 address to be used while applying the configuration** — **Prompt the user for IPv6 address if no default is available**

Export Host Customizations

You can export the customized attributes of a host profile as a `.csv` file on your desktop.

For security, sensitive data such as passwords are not exported.

1. Navigate to **Hosts and Clusters** and select a ESXi host with an attached host profile.
2. Right-click the ESXi host and select **Host Profiles** > **Export Host Customizations**.
3. Click **Save**.

   Note: Only English version of the `.csv` file is supported.

   The file is saved as a `.csv` file.

After the file is saved to your desktop, you can manually edit the file and save it to apply the customizations later.

Edit Host Customizations

You can edit the host customizations for specific hosts attached to a host profile or cluster attached to a host profile.

1. Navigate to **Hosts and Clusters** and select an ESXi host with an attached host profile.
2. Right-click the host profile and select **Edit Host Customizations**.
3. Select the host or hosts of which you want to edit the customizations, and click **Next**.
4. Optional: In the **Customize hosts** page, you can **Import Host Customization** `.csv` file from your desktop.

   If you want to edit host customizations by using a `.csv` file, you can export the host customizations in `.csv` file format, edit the values in the answer file fields, and then import the file. For more information on how to export host customizations, see Export Host Customizations.

   Note: User input in the **Customize hosts** pane is overwritten by the import process and the values from the `.csv` file.

   After importing the `.csv` file, the text boxes are updated with the information from the file.
5. Edit the host configuration values.
6. Click **Finish**.

Configure Security Host Profile

Use this procedure to manage role, user account, and active directory permission profiles that are grouped as part of the security host profile.

Make sure that you have the SecurityConfigProfile plugin available to validate the role, user account, and active directory permission profiles as there are dependencies between them.

You can configure the host profile options, part of the security profile.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Unfold the **Security and Services** > **Security Settings** profile category and open the **Security** folder.

   You are present with the following profiles:

Role	This profile allows you to view default roles and add custom roles within the ESXi system.
User Configuration	This profile allows you to create and manage user accounts. Here are some of the operations that you can perform for user accounts: • Create a user account.

	• Configure the password for a user account. • Configure the password for the root user. • Configure the role for any user that is not the default one. • Assign a default or custom role (configure permissions) for a local account. • Configure the SSH key for any user.
Active Directory Permission	This profile allows you to manage permissions for active directory users or groups. For example, you can create permissions that associate an active directory user or a group with a role. When an ESXi host joins the active directory domain, an Admin permission is created for the DOMAIN group **ESX Admins**. Also, when an active directory user or group is given some permissions on the ESXi host, a corresponding permission is created on that host. The Active Directory Permission profile captures that permission.
Lockdown Mode	This profile allows you to increase the security of your ESXi hosts by restricting user permissions and privileges. You can configure the following lockdown mode settings: • Normal lockdown mode: An ESXi host can be accessed from a local console and vCenter Server. DCUI service is not stopped. • Strict lockdown mode: An ESXi host can be only accessed from vCenter Server. DCUI service is stopped. • Exception users: The users that still have their permissions regardless of the lockdown mode state.

For more information on the security profile, see the *vSphere Security* documentation.

Configure Networking Host Profiles

By default, hosts provisioned with vSphere Auto Deploy are assigned DHCP addresses by a DHCP server. You can use the vSphere Auto Deploy host customization mechanism to assign static IP addresses to hosts.

- Set up your vSphere Auto Deploy environment.

- Boot the host using vSphere Auto Deploy.
- Extract a host profile from the host.

1. In the vSphere Client, select **Menu** > **Policies and Profiles**.
2. Change the default IP address settings by locating **Networking configuration** > **Host port group** > **Management Network** > **IP address settings**.
3. From the **IPv4 address** drop-down menu, select **User specified IP address to be used while applying the configuration**.
4. If the host is in a different subnet than the vCenter Server system, select **Networking Configuration** > **NetStack Instance** > **defaultTcpipStack** > **DNS configuration** and enter the default route in the **Default IPv4 gateway** text box.
5. Select **Networking Configuration** > **NetStack Instance** > **defaultTcpipStack** > **DNS configuration**.
6. Make sure the **Flag indicating if DHCP should be used** check box is deselected.
7. Right-click the host and select **All vCenter Actions** > **Host Profiles** > **Attach Host Profile**.
8. Select the profile to attach and click **Next**.
9. Provide the IP address and net mask and click **Finish**.
10. Reboot the ESXi host.

The IP address is saved as a host customization and applied to the host.

Recommended Host Profiles Upgrade Workflows

Each workflow is the recommended upgrade path while upgrading your vCenter Server 6.5 and 6.7 environment, that contains one or more host profiles with version 6.0, 6.5 and 6.7.

Upgrade Support Matrix

When you upgrade your vCenter Server from version 6.5 or 6.7 to version 7.0, you can keep your current ESXi host version and Host Profiles version. For other upgrade workflows, see the *Upgrade Support Matrix*.

Note: vCenter Server version 6.0 and ESXi 5.5 hosts are not supported in vCenter Server7.0. You can use the *Recommended Host Profiles Upgrade Workflows* in the vSphere Host Profiles 6.7 guide as intermediate upgrade steps.

Table 178: Upgrade Support Matrix

Upgrade Workflow	vCenter Server	ESXi host	Host Profiles
earlier than 5.5 -> 6.0 / 6.5 -> 6.7	Requires an upgrade	Requires an upgrade	Requires an upgrade
5.5 -> 6.7	Requires an upgrade	Requires an upgrade	Requires an upgrade
6.0 -> 6.7	Requires an upgrade	An optional upgrade	An optional upgrade
6.5 -> 7.0	Requires an upgrade	An optional upgrade	An optional upgrade
6.7 -> 7.0	Requires an upgrade	An optional upgrade	An optional upgrade
earlier than 6.5 -> 6.5 / 6.7 -> 7.0	Requires an upgrade	Requires an upgrade	Requires an upgrade
6.5/6.7/7.0 →7.0 Update 3	Requires an upgrade	An optional upgrade	An optional upgrade

Upgrade Workflow	vCenter Server	ESXi host	Host Profiles
		Note: You might need to keep a 7.0 GA host if you want to validate or edit a 7.0 GA host profile.	

vCenter Server and ESXi Version Interoperability

Starting with vSphere 7.0 Update 3, a major-version vCenter Server instance supports any ESXi Update release version of the corresponding major release. That is, a vCenter Server 7.0 Update 3 instance can manage ESXi 6.5, ESXi 6.7, and any Update release of ESXi 7.0.

So, you must upgrade vCenter Server to 7.0 Update 3, if you want to manage ESXi hosts of version 7.0 Update 3 or a later Update release. You must also upgrade vCenter Server to version 7.0 Update 3 if you want to manage a mixed environment of hosts of any ESXi 7.0 Update release version, for example 7.0 GA, 7.0 Update 1, or 7.0 Update 2.

vCenter Server Upgrade from 6.5 to 7.0 With Stateful ESXi Hosts Version 6.5 or Earlier

Use the upgrade workflows to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 7.0.

Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi6.0 and 6.5 Hosts

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 7.0, if your cluster contains stateful ESXi6.0 and 6.5 hosts.

Prerequisites

- Verify that your cluster contains ESXi6.0 and ESXi 6.5 hosts.
- Verify that a host profile with version 6.0 is attached to the cluster.
- Verify that your vCenter Server is with version 6.5.

Procedure

1. Upgrade all ESXi6.0 hosts in the cluster to version 6.5.
   For more information, see the *VMware ESXi Upgrade* documentation.
2. Remediate the upgraded hosts against the host profile with version 6.0.
   During remediation, all host profile settings are applied to the hosts in the cluster.
3. Extract a new host profile from an ESXi 6.5 host in the cluster.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
4. Attach the host profile with version 6.5 to the cluster.
5. Remediate the cluster against the host profile with version 6.5.
6. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.
7. Upgrade all ESXi hosts in the cluster to version 7.0.
   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534

8. Remediate the cluster against the host profile with version 6.5.
   During remediation, all host profile settings are applied.
9. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
10. Attach the host profile with version 7.0 to the cluster.
    The host customization data updates automatically.
    All host profile operations become available.

Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi 6.5 Hosts Only

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 7.0, if your cluster contains stateful ESXi 6.5 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.5 hosts only.
- Verify that a host profile with version 6.5 is attached to the cluster.
- Verify that your vCenter Server is with version 6.5.

Procedure

1. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.
2. Upgrade all ESXi hosts in the cluster to version 7.0.
   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534
3. Remediate the cluster against the host profile with version 6.5.
   During remediation, all host profile settings are applied.
4. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
5. Attach the host profile with version 7.0 to the cluster.
   The host customization data updates automatically.
   All host profile operations become available.

vCenter Server Upgrade from 6.7 to 7.0 With Stateful ESXi Hosts Version 6.7 or Earlier

Use the upgrade workflows to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 7.0.

Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi6.0, 6.5, and 6.7 Hosts

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 7.0, if your cluster contains stateful ESXi6.0, ESXi 6.5, and ESXi6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi6.0, 6.5, and ESXi6.7 hosts.
- Verify that a host profile with version 6.0 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.

Procedure

1. Upgrade all ESXi6.0 hosts in the cluster to version 6.7.
   For more information, see the *VMware ESXi Upgrade* documentation.
2. Remediate the upgraded hosts against the host profile with version 6.0.
   During remediation, all host profile settings are applied to the hosts in the cluster.
3. Extract a new host profile from an ESXi 6.5 or 6.7 host in the cluster.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
4. Attach the host profile with version 6.5 or 6.7 to the cluster.
5. Remediate the cluster against the host profile with version 6.5 or 6.7.
6. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.
7. Upgrade all ESXi hosts in the cluster to version 7.0.
   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534
8. Remediate the cluster against the host profile with version 6.5 or 6.7.
   During remediation, all host profile settings are applied.
9. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
10. Attach the host profile with version 7.0 to the cluster.
    The host customization data updates automatically.
    All host profile operations become available.

Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi 6.5 and 6.7 Hosts

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 7.0, if your cluster contains stateful ESXi 6.5 and 6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.5 and ESXi6.7 hosts.
- Verify that a host profile with version 6.5 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.

Procedure

1. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.

2. Upgrade all ESXi hosts in the cluster to version 7.0.
   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534
3. Remediate the cluster against the host profile with version 6.5.
   During remediation, all host profile settings are applied.
4. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
5. Attach the host profile with version 7.0 to the cluster.
   The host customization data updates automatically.
   All host profile operations become available.

Upgrading Host Profiles in a vCenter Server Environment with Stateful ESXi6.7 Hosts Only

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 7.0, if your cluster contains stateful ESXi6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi6.7 hosts only.
- Verify that a host profile with version 6.7 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.

Procedure

1. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.
2. Upgrade all ESXi hosts in the cluster to version 7.0.
   Edit host customization and host profile edit operations are not available, while compliance check, attach host profile, and remediate hosts operations are available. For more information, see KB 2150534
3. Remediate the cluster against the host profile with version 6.7.
   During remediation, all host profile settings are applied.
4. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
5. Attach the host profile with version 7.0 to the cluster.
   The host customization data updates automatically.
   All host profile operations become available.

vCenter Server Upgrade from 6.5 to 7.0 in an Environment with Stateless ESXi 6.5 Hosts Only

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.5 to version 7.0, if your cluster contains stateless ESXi 6.5 hosts.

Prerequisites

- Verify that your cluster contains ESXi 6.5 hosts only.

- Verify that a host profile with version 6.5 is attached to the cluster.
- Verify that your vCenter Server is with version 6.5.

Procedure

1. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.
2. Create a new rule or edit the existing rule with an image profile version 7.0 and select the cluster.
3. Remediate all ESXi hosts in the cluster by clicking **Remediate Host Associations**.
4. Reboot all ESXi hosts in the cluster.
   All hosts are compliant with the host profile version 6.5, but the host profile cannot be edited. Remediation and check compliance operations are available.

What to do next

To be able to customize your host profile, follow these steps.

1. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
2. Attach the host profile with version 7.0 to the cluster.
   The host customization data updates automatically.
   All host profile operations become available.

vCenter Server Upgrade from 6.7 to 7.0 in an Environment With Stateless ESXi6.7 Hosts Only

You use the present workflow to resolve version compliance errors when upgrading vCenter Server with version 6.7 to version 7.0, if your cluster contains stateless ESXi6.7 hosts.

Prerequisites

- Verify that your cluster contains ESXi6.7 hosts only.
- Verify that a host profile with version 6.7 is attached to the cluster.
- Verify that your vCenter Server is with version 6.7.

Procedure

1. Upgrade your vCenter Server instance to version 7.0.
   The vCenter Server configuration is not changed during the upgrade.
   For more information, see the *vCenter Server Upgrade* documentation.
2. Create a new rule or edit the existing rule with an image profile version 7.0 and select the cluster.
3. Remediate all ESXi hosts in the cluster by clicking **Remediate Host Associations.**
4. Reboot all ESXi hosts in the cluster.
   All hosts are compliant with the host profile version 6.7, but the host profile cannot be edited. Remediation and check compliance operations are available.

What to do next

To be able to customize your host profile, follow these steps.

1. Extract a new host profile from an ESXi7.0 host.
   During host profile extraction, some parameters of the configured host profile policy change. For more information, see Answer File Field and Host Profile Extraction.
2. Attach the host profile with version 7.0 to the cluster.
   The host customization data updates automatically.
   All host profile operations become available.

Using Host Profiles to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch

Starting with vSphere 7.0, the vSphere Distributed Switch supports the NSX functionality. For clusters enabled with VMware NSX-T Data Center™, you can use the regular ESXi upgrade workflow to migrate the NSX-managed Virtual Distributed Switches of the hosts to vCenter Server-managed vSphere Distributed Switches. By using host profiles, you can perform the upgrade and the host switch migration in an environment where all hosts are provisioned with Auto Deploy.

Migrating your host switch to vSphere Distributed Switch 7.0 ensures optimal pNIC usage, and lets you manage the networking for your NSX hosts from vCenter Server.

Requirements

- Verify that the ESXi hosts to upgrade are version 6.7 or later.
- vCenter Server 7.0 Update 2
- VMware NSX-T Data Center™ 3.1.1

As a good practice, contact VMware support to assess the impact of migrating to vSphere Distributed Switch 7.0.

Workflow

1. Upgrade vCenter Server to version 7.0 Update 2.
   For more information about upgrading , see the *vSphere Upgrade* documentation.
2. Upload a software depot that contains an ESXi 7.0 Update 2 image. to vCenter Server.
   For more information, see the *VMware ESXi Installation and Setup* documentation.
3. In NSX Manager, run the migration readiness pre-check, address any configuration issues, review the recommended topology, and create a vSphere Distributed Switch.
   Note: At this point, do not make any configuration changes to VMware NSX-T Data Center™.
   For more information about the steps you need to perform in NSX Manager, see "Migrate Host Switch to vSphere Distributed Switch" in the *NSX-T Data Center Administration* documentation.
4. Create a new image rule or update the existing one with the uploaded ESXi 7.0 Update 2 image.
   For more information, see the *VMware ESXi Installation and Setup* documentation.
5. Reboot the reference host.
   The reboot triggers the migration of the host switches from NSX Virtual Distributed Switches to vSphere Distributed Switches.
   After the reboot, the ESXi version on the reference host is upgraded to 7.0 Update 2. A new TNP with vSphere Distributed Switch is attached to the cluster.
6. Update the host profile by copying the settings from the reference host.
   The updated host profile is configured with vSphere Distributed Switch instead of NSX Virtual Distributed Switch.
   For more information, see Copy Settings from Host.

7. Reboot all ESXi hosts in the cluster.
   After the reboot, all hosts in the cluster use the new host profile, which is configured with vSphere Distributed Switch instead of NSX Virtual Distributed Switch.

Answer File Field and Host Profile Extraction

There are changes in thehost profiles policy options and host customization values, when a new profile is extracted from a host (or post upgrade). You can get more familiar with those changes by referring to the Answer File Field and Host Profile Extraction table.

After you extract a new host profile from an ESXi host, the values for some of the policy options change. To keep these values, you have to save them manually before extracting the host profile. The *Answer File Field and Host Profile Extraction* table lists the policy options with changed values as well as the options that keep their values the same in the newly extracted host profile.

To locate the policy options, navigate to **Host Profiles** main view, right-click the extracted host profile and select **Edit Host Customizations.**

Table 179: Answer File Field and Host Profile Extraction

Policy option path	Policy option	Variations in the policy options value in the newly extracted profile
Security and Services -> Security Settings -> Security	UserInputPasswordConfigOption	For default users, it leaves the password unchanged (root). For non-default users, it always extracts user input.
	UserInputPasswordConfigOption	If host profile version is earlier than 6.7, this option is not extracted. You explicitly need to create a UserAccount profile in the extracted host profile.
	UserInputAdminPasswordOption	Changes to fixed. Does not keep user input value.
Storage configuration -> iSCSI Initiator Configuration	AdvancedUserInputUserConfigOption	Changes to fixed. Does not keep user input value.
	UserInputIqn	Keeps user input value.
	UserInputAlias	Keeps user input value.
	UserInputChapName	Changes to fixed. Does not keep user input value.
	UserInputChapSecret	Changes to fixed. Does not keep user input value.
	UserInputFirstBurstLength	Changes to fixed. Does not keep user input value.
	UserInputMaxBurstLength	Changes to fixed. Does not keep user input value.
General System Settings -> Management Agent Configuration -> SNMP Agent Configuration	UserInputMaxReceiveSegmentLength	Changes to fixed. Does not keep user input value.
	UserInputUsers	Changes to fixed. Does not keep user input value.
	UserInputV3Targets	Changes to fixed. Does not keep user input value.
	UserInputEngineId	Changes to fixed. Does not keep user input value.
	UserInputContact	Changes to fixed. Does not keep user input value.
	UserInputLocation	Changes to fixed. Does not keep user input value.
Security and Services -> Security Settings -> Security -> Active Directory Permission	UserInputUserName	Keeps user input value.
	UserInputPassword	Keeps user input value.

Policy option path	Policy option	Variations in the policy options value in the newly extracted profile
Networking Configuration	UserInputMacAddress	Conditional, prompt user if no default value is available.
	UserInputHostName	Conditional, prompt user if no default value is available.
	UserInputIPAddress	Conditional, prompt user if no default value is available.
Advanced Configuration Settings -> Advanced Options	UserInputAdvancedConfigOption	Changes to fixed. Does not keep user input value.
Advanced Configuration Settings -> System Image Cache Configuration	Enable Stateless Caching	You must explicitly select the policy option.
	Enable Stateful Install	You must explicitly select the policy option.

Note: This table does not list all policy options. You must be aware of the policy options you modified before extracting a new host profile.

Troubleshooting Host Profiles

The Host Profiles troubleshooting topics provide solutions to problems that you might encounter when performing tasks for Host Profiles in vCenter Server .

If upgrading your vCenter Server to version 7.0 results with a failure due to an existing host profile in the inventory, see *vCenter Server Upgrade* for Upgrade Issues with vCenter Server Containing Host Profiles.

Host Customization Data Is Missing

Deploying a stateless host results with a failure in exiting maintenance mode.

When you are in the process of deploying a stateless host, the host fails in exiting maintenance mode.

In an environment where the following takes place for a host profile:

- The host profile is attached to a stateless host.
- The host profile has host-specific settings.

When the stateless host is rebooting, applying the host profile fails because the host does not exit from a maintenance mode.

- Provide a host customization as described in Edit Host Customizations.
- Remediate the host profile to the host again.
- Reboot the host, if needed.
- Refer to the host profiles command-line utility in Host Profiles CLI for customizing stateless hosts.

Reference Host is Unavailable

Creating a Host Profile into the vCenter Server inventory results with a failure.

When you perform Host Profiles operations into the vCenter Server inventory such as:

- Edit a Host Profile.
- Import a Host Profile.
- Export a Host Profile.

The process of creating a host profile fails with an error.

```
There is no suitable host in the inventory as reference host for the profile Host Profile. The profile does
 not have any associated reference host.
```

The vCenter Server inventory does not have a compatible host that acts as a reference host for the host profile you are trying to create.

Add a host that acts as a reference host in the vCenter Server inventory with the same version as the host profile you are trying to create.

Compliance Failures with Storage Host Profiles

When you use storage devices, that are not shared across a cluster, but the vSphere storage stack cannot detect them as local (for example, some SAS devices), applying a host profile might result with compliance failures.

To resolve the compliance failures caused by using local storage devices, use the upgraded Pluggable Storage Architecture (PSA) host profile policies.

To find out whether a device is detected as local or not, you can check the **Is Local** setting for a device by running the command `esxcli storage core device list -d naa.xxxx` in the ESXi shell. For more information on this command and identifying disks or LUNs, see KB 1014953.

Note: ESXi diagnostic data that you obtain by running the `vm-support` command contains host profiles information which includes storage host profiles, PSA, NMP, and Virtual Volumes data. No sensitive information, such as passwords, is collected.

Compliance Failures with Serial Attached SCSI (SAS) Devices

This procedure resolves compliance failures for SAS devices that are not detected as local by the vSphere storage stack.

Extract a host profile from a reference host. See Create a Host Profile for instructions.

1. Navigate to **Host Profiles** main view and select the host profile that you want to edit.
2. Click the Configure tab and click **Edit Host Profile**.
3. Select **Storage configuration** > **Pluggable Storage Architecture configuration** > **PSA device sharing** > ***name of device***
4. For each device not shared across the cluster, disable **Device is shared clusterwide**.

   Note: By default, the **Device is shared clusterwide** setting is disabled for devices detected as local and enabled for non-local devices. This setting allows storage host profiles to ignore local devices during compliance checks.

   The **Device is Shared Clusterwide** setting for PSA devices helps you determine which devices in the cluster should be configured by a host profile. Correctly setting this value for devices in the cluster eliminates compliance errors due to non-shared devices.
5. Remediate the host profile to the reference host for the changes to take effect.

Compliance failures with SAN Boot LUN Devices

This procedure resolves compliance failures for SAN boot LUN devices shared across the cluster, but logically local to the ESXihost.

Extract a host profile from a reference host. See Create a Host Profile for instructions.

To avoid this compliance failure from occurring, set the **Device is shared clusterwide** value to **False** before extracting the host profile from the reference host. You can disable the value by using the command `esxcli storage core device`

`setconfig -d naa.xxxx --shared-clusterwide=false`, where *`naa.xxxx`* is the unique device identifier generated in naa format.

1. Navigate to **Host Profiles** main view and select the host profile that you want to edit.
2. Click the Configure tab and click **Edit Host Profile**.
3. Select **Storage configuration** > **Pluggable Storage Architecture configuration** > **PSA device sharing** > ***name of device***
4. Disable the **Device is shared clusterwide** in the host profile by deselecting the check box.

   When applying the host profile to the target host, the boot device settings for the remote boot LUN device are copied from the reference host into the target host.
5. Optional:
6. Optional: Select **Storage configuration** > **Pluggable Storage Architecture configuration** > **Host boot device configuration** and verify that the boot LUN ID is correctly captured.
7. Remediate the host profile to the reference host for the changes to take effect.

   If you must re-extract the host profile (for example, if you attach more shared SAN boot LUNs to your cluster), you do not need to reconfigure the **Device is Shared Clusterwide** setting for devices that you previously configured via esxcli.

Edit Settings for Host Profiles is Failing

Editing a host profile results with an error.

In a vCenter Server inventory upgraded to version 6.5 if you try to edit the settings for a host profile with version 5.1, one of the following errors might appear:

```
Unexpected status code: 503
```

or

```
There are no hosts available in the inventory at the version for the selected Host Profile
```

vSphere 6.5 supports only hosts and host profiles with version 5.5 and later.

- Extract a Host Profile from an already upgraded host to version 5.5. or later.
- Use the **Copy Settings from Host** option to copy the configuration settings from a host already upgraded to a version 5.5. or later.

  Note: Using the **Copy Settings from Host** option overwrites the settings within the existing Host Profile or sets them to the default values.

Host Profile without NFS Datastore

Host profile compliance check fails for NFS datastore.

When you confirm the compliance of your ESXi host to its attached Host Profile, a non-compliant status is present for the NFS datastore. The compliance check detects the mounted NFS datastore to the ESXi host as an additional datastore.

The remediate or compliance check failure occurs when the following two conditions take place:

- The extracted Host Profile does not have NFS storage (NasStorageProfile).

- The ESXi host, attached to the Host Profile, has an already mounted NFS storage.

1. Create a dummy NFS datastore in the Host Profile.
2. Disable the dummy NFS datastore so that the NFS storage profile is fully disabled.

Upgraded Host is Not Compliant with a Legacy Host Profile

An upgraded ESXi host with attached legacy host profile results with a non-compliant status after reboot.

When you upgrade a host to the latest ESXi version and remediate the attached legacy host profile to that host, the compliance status might be updated to non-compliant after the host reboots.

You are using a legacy host profile, which is attached to an ESXi host version 6.7 or earlier and contains the following sub-profiles:

- `Misc.LogPort`
- `host/vim/vmvisor/plugins/vmware_*`

- Make the ESXi host compliant with the legacy host profile.
  a. From the **Host Profiles** main view, right-click the host profile that you want to edit and select **Edit Host Profile**.
  b. In the **Edit host profile** page, disable the sub-profile(s).
  c. **Check Host Profile Compliance**.
- Upgrade the legacy host profile to the same version as the ESXi host.
  a. Right-click the legacy host profile and select **Copy Settings from Host**.
  b. Select the upgraded ESXi host from which you want to copy the configuration settings and click **OK**.

vSphere Networking

vSphere Networking provides information about configuring networking for VMware vSphere®, including how to create vSphere distributed switches and vSphere standard switches.

vSphere Networking also provides information on monitoring networks, managing network resources, and networking best practices.

Intended Audience

The information presented is written for experienced Windows or Linux system administrators who are familiar with network configuration and virtual machine technology.

vSphere Web Client and vSphere Client

Instructions in this guide reflect the vSphere Client (an HTML5-based GUI). You can also use the instructions to perform the tasks by using the vSphere Web Client (a Flex-based GUI).

Tasks for which the workflow differs significantly between the vSphere Client and the vSphere Web Client have duplicate procedures that provide steps according to the respective client interface. The procedures that relate to the vSphere Web Client, contain vSphere Web Client in the title.

Note: In vSphere 6.7 Update 1, almost all of the vSphere Web Client functionality is implemented in the vSphere Client. For an up-to-date list of any remaining unsupported functionality, see Functionality Updates for the vSphere Client.

Updated Information

This *vSphere Networking* is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Networking*.

Revision	Description
11 MAY 2022	Added a note about prefix- based MAC address. See Prefix-Based MAC Address Allocation.
28 MAR 2022	Added a description for explicit congestion notification. See Explicit Congestion Notification .
25 MAR 2022	Updated a note about a fast timeout. See Edit a Link Aggregation Group.
25 JAN 2022	Added a note about limitations when selecting port mirroring sources. See Select Port Mirroring Sources.
05 OCT 2021	Initial release.

Introduction to vSphere Networking

Get to know the basic concepts of vSphere networking and how to set up and configure a network in a vSphere environment.

Networking Concepts Overview

A few concepts are essential for a thorough understanding of virtual networking. If you are new to vSphere, it is helpful to review these concepts.

Physical Network	A network of physical machines that are connected so that they can send data to and receive data from each other. VMware ESXi runs on a physical machine.
Virtual Network	A network of virtual machines running on a physical machine that are connected logically to each other so that they can send data to and receive data from each other. Virtual machines can be connected to the virtual networks that you create when you add a network.
Opaque Network	An opaque network is a network created and managed by a separate entity outside of vSphere. For example, logical networks that are created and managed by VMware NSX® appear in vCenter Server as opaque networks of the type nsx.LogicalSwitch. You can choose an opaque network as the backing for a VM network adapter. To manage an opaque network, use the management tools associated with the opaque network, such as VMware NSX® Manager or the VMware NSX API management tools. **Note:** With NSX-T 3.0, it is now possible to run NSX-T directly on vSphere Distributed Switch (vDS) version 7.0 or later. Such networks are not opaque, and are identified as NSX logical segments running on vDS 7.0. For more information, see Knowledge Base article KB #79872.
Physical Ethernet Switch	A physical ethernet switch manages network traffic between machines on the physical network. A switch has multiple ports, each of which can be connected to a single machine or another switch on the network. Each port can be configured to behave in certain ways depending on the needs of the machine connected to it. The switch learns which hosts are connected to which of its ports and uses that information to forward traffic to the correct physical machines. Switches are the core of a physical network. Multiple switches can be connected together to form larger networks.
vSphere Standard Switch	It works much like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. A vSphere standard switch can be connected to physical switches by using physical Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks. This type of connection is similar to connecting physical switches together to create a larger network. Even though a vSphere standard switch works much like a physical switch, it does not have some of the advanced functionality of a physical switch.
vSphere Distributed Switch	A vSphere distributed switch acts as a single switch across all associated hosts in a data center to provide centralized provisioning, administration, and monitoring of virtual networks. You configure a vSphere distributed switch on the vCenter Server system and the configuration is propagated to all hosts that are associated with the switch. This lets virtual machines maintain consistent network configuration as they migrate across multiple hosts.
Host Proxy Switch	A hidden standard switch that resides on every host that is associated with a vSphere distributed switch. The host proxy switch replicates the networking configuration set on the vSphere distributed switch to the particular host.
Standard Port Group	Network services connect to standard switches through port groups. Port groups define how a connection is made through

	the switch to the network. Typically, a single standard switch is associated with one or more port groups. A port group specifies port configuration options such as bandwidth limitations and VLAN tagging policies for each member port.
Distributed Port	A port on a vSphere distributed switch that connects to a host's VMkernel or to a virtual machine's network adapter.
Distributed Port Group	A port group associated with a vSphere distributed switch that specifies port configuration options for each member port. Distributed port groups define how a connection is made through the vSphere distributed switch to the network.
NSX Distributed Port Group	A port group associated with a vSphere distributed switch that specifies port configuration options for each member port. To distinguish between vSphere distributed port groups and NSX port groups, in the vSphere Client the NSX virtual distributed switch, and its associated port group, is identified with the icon. NSX appears as an opaque network in vCenter Server, and you cannot configure NSX settings in vCenter Server. The NSX settings displayed are read only. You configure NSX distributed port groups using VMware NSX® Manager or the VMware NSX API management tools. To learn about configuring NSX, see the *NSX Data Center for vSphere* documentation.
NSX Manager Appliance Plug-in	NSX Manager Appliance can be installed from the vSphere Web Client. You do not need to perform any installation operations from the NSX Manager UI. After the NSX Manager is installed, NSX appears as a plug-in in the vCenter Server that is ready to install NSX-T for virtual networking or security use cases. For more information, see the *VMware NSX-T Data Center* documentation. This functionality is available on VMware vSphere 7.0 Update 3 and later and VMware NSX-T Data Center 3.2 and later.
NIC Teaming	NIC teaming occurs when multiple uplink adapters are associated with a single switch to form a team. A team can either share the load of traffic between physical and virtual networks among some or all of its members, or provide passive failover if there is a hardware failure or a network outage.
VLAN	VLAN enable a single physical LAN segment to be further segmented so that groups of ports are isolated from one another as if they were on physically different segments. The standard is 802.1Q.
VMkernel TCP/IP Networking Layer	The VMkernel networking layer provides connectivity to hosts and handles the standard infrastructure traffic of vSphere vMotion, IP storage, Fault Tolerance, and vSAN.
IP Storage	Any form of storage that uses TCP/IP network communication as its foundation. iSCSI and NFS can be used as virtual machine datastores and for direct mounting of `.ISO` files, which are presented as CD-ROMs to virtual machines.
TCP Segmentation Offload	TCP Segmentation Offload, TSO, allows a TCP/IP stack to emit large frames (up to 64KB) even though the maximum transmission unit (MTU) of the interface is smaller. The network adapter then separates the large frame into MTU-sized frames and prepends an adjusted copy of the initial TCP/IP headers.

Network Services in ESXi

A virtual network provides several services to the host and virtual machines.

You can enable two types of network services in ESXi:

- Connecting virtual machines to the physical network and to each other.

- Connecting VMkernel services (such as NFS, iSCSI, or vMotion) to the physical network.

VMware ESXi Dump Collector Support

The ESXi Dump Collector sends the state of the VMkernel memory, that is, a core dump to a network server when the system encounters a critical failure.

The ESXi Dump Collector in ESXi supports both vSphere Standard and Distributed Switches. The ESXi Dump Collector can also use any active uplink adapter from the team of the port group that handles the VMkernel adapter for the collector.

Changes to the IP address for the ESXi Dump Collector interface are automatically updated if the IP addresses for the configured VMkernel adapter changes. The ESXi Dump Collector also adjusts its default gateway if the gateway configuration of the VMkernel adapter changes.

If you try to delete the VMkernel network adapter used by the ESXi Dump Collector, the operation fails and a warning message appears. To delete the VMkernel network adapter, deactivate dump collection and delete the adapter.

There is no authentication or encryption in the file transfer session from a crashed host to the ESXi Dump Collector. You should configure the ESXi Dump Collector on a separate VLAN when possible to isolate the ESXi core dump from regular network traffic.

For information about installing and configuring the ESXi Dump Collector, see the *vCenter Server Installation and Setup* documentation.

Setting Up Networking with vSphere Standard Switches

vSphere standard switches handle network traffic at the host level in a vSphere deployment.

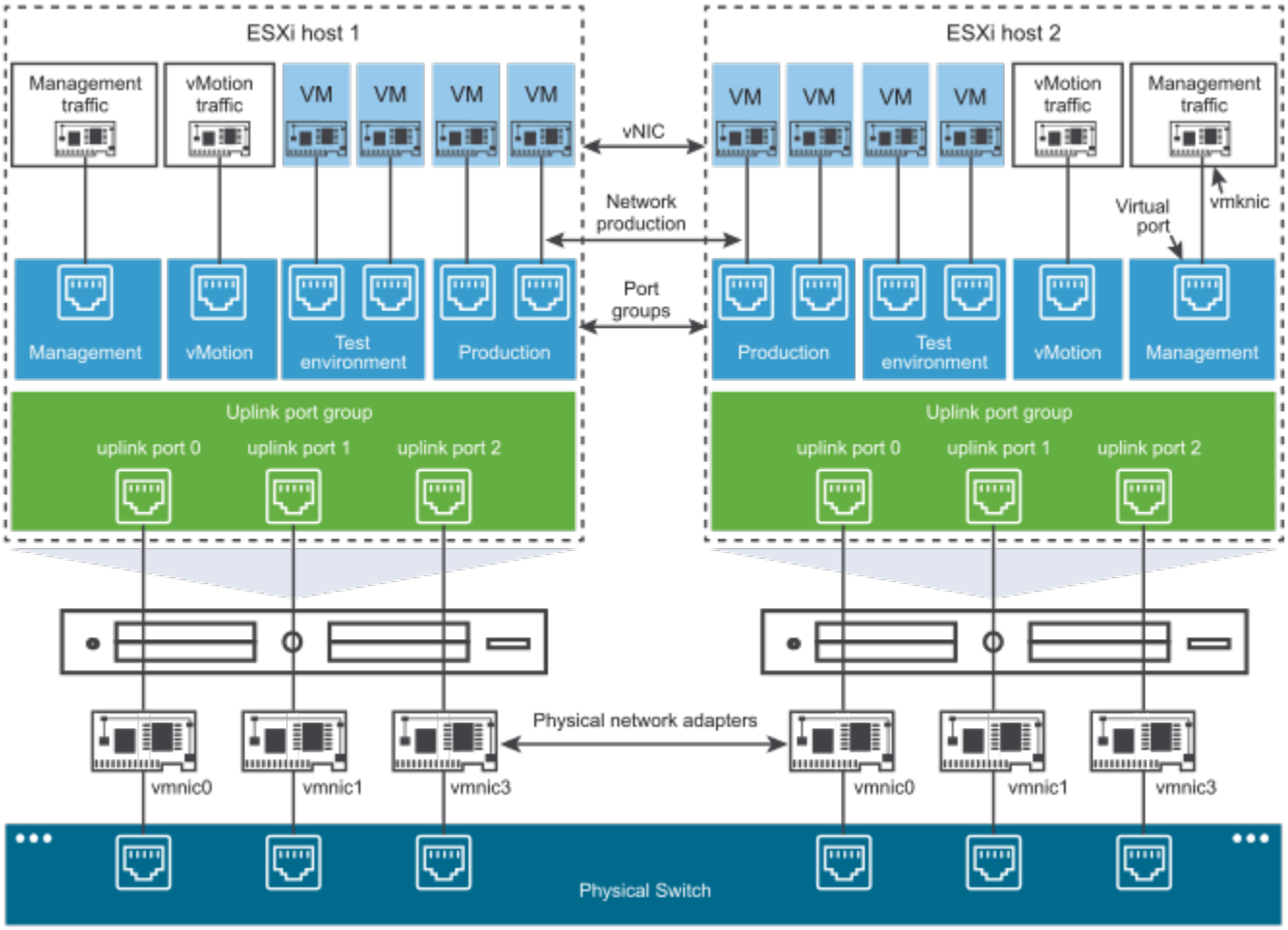
vSphere Standard Switches

You can create abstracted network devices called vSphere Standard Switches. You use standard switches to provide network connectivity to hosts and virtual machines. A standard switch can bridge traffic internally between virtual machines in the same VLAN and link to external networks.

Standard Switch Overview

To provide network connectivity to hosts and virtual machines, you connect the physical NICs of the hosts to uplink ports on the standard switch. Virtual machines have network adapters (vNICs) that you connect to port groups on the standard switch. Every port group can use one or more physical NICs to handle their network traffic. If a port group does not have a physical NIC connected to it, virtual machines on the same port group can only communicate with each other but not with the external network.

Figure 49: vSphere Standard Switch architecture



A vSphere Standard Switch is very similar to a physical Ethernet switch. Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port. Each logical port on the standard switch is a member of a single port group. For information about maximum allowed ports and port groups, see the *Configuration Maximums* documentation.

Standard Port Groups

Each port group on a standard switch is identified by a network label, which must be unique to the current host. You can use network labels to make the networking configuration of virtual machines portable across hosts. You should give the same label to the port groups in a data center that use physical NICs connected to one broadcast domain on the physical network. Conversely, if two port groups are connected to physical NICs on different broadcast domains, the port groups should have distinct labels.

For example, you can create `Production` and `Test environment` port groups as virtual machine networks on the hosts that share the same broadcast domain on the physical network.

A VLAN ID, which restricts port group traffic to a logical Ethernet segment within the physical network, is optional. For port groups to receive the traffic that the same host sees, but from more than one VLAN, the VLAN ID must be set to VGT (VLAN 4095).

Number of Standard Ports

To ensure efficient use of host resources on ESXi hosts, the number of ports of standard switches are dynamically scaled up and down. A standard switch on such a host can expand up to the maximum number of ports supported on the host.

Create a vSphere Standard Switch

Create a vSphere Standard Switch to provide network connectivity for hosts, virtual machines, and to handle VMkernel traffic. Depending on the connection type that you want to create, you can create a new vSphere Standard Switch with a VMkernel adapter, only connect physical network adapters to the new switch, or create the switch with a virtual machine port group.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual switches**.
3. Click **Add networking**.
4. Select a connection type for which you want to use the new standard switch and click **Next**.

Option	Description
VMkernel Network Adapter	Create a new VMkernel adapter to handle host management traffic, vMotion, network storage, fault tolerance, or vSAN traffic.
Physical Network Adapter	Add physical network adapters to an existing or a new standard switch.
Virtual Machine Port Group for a Standard Switch	Create a new port group for virtual machine networking.

5. Select **New standard switch** and click **Next**.
6. Add physical network adapters to the new standard switch.
   a) Under Assigned adapters, click **Add adapters**.
   b) Select one or more physical network adapters from the list and click **OK**.

      For higher throughput and to provide redundancy, configure at least two physical network adapters in the Active list.
   c) Optional: Use the **Move up** and **Move down** arrows in the **Assigned adapters** list to change the position of the adapter.
   d) Click **Next**.
7. If you create the new standard switch with a VMkernel adapter or virtual machine port group, enter connection settings for the adapter or the port group.

Option	Description
VMkernel adapter	1. Enter a label that indicates the traffic type for the VMkernel adapter, for example `vMotion`. 2. Set a VLAN ID to identify the VLAN that the network traffic of the VMkernel adapter will use. 3. Select IPv4, Ipv6 or both. 4. Select an option from the drop-down menu to set the MTU size. If you select Custom, enter a value for the MTU size. You can enable jumbo frames by setting an MTU value greater than 1500. You cannot set an MTU size greater than 9000 bytes. 5. Select a TCP/IP stack. After you set a TCP/IP stack for the VMkernel adapter, you cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you will be able to use only this stack to handle vMotion or Provisioning traffic on the host.

Option	Description
	6. If you use the default TCP/IP stack, select from the available services. 7. Configure IPv4 and IPv6 settings.
Virtual machine port group	1. Enter a network Label or the port group, or accept the generated label. 2. Set the VLAN ID to configure VLAN handling in the port group.

8. On the Ready to Complete page, click **Finish**.

- You might need to change the teaming and failover policy of the new standard switch. For example, if the host is connected to an Etherchannel on the physical switch, you must configure the vSphere Standard Switch with Route based on IP hash as a load balancing algorithm. See Teaming and Failover Policy for more information.
- If you create the new standard switch with a port group for virtual machine networking, connect virtual machines to the port group.

Related Links

VMkernel Networking Layer on page 2192

The VMkernel networking layer provides connectivity to hosts and handles the standard system traffic of vSphere vMotion, IP storage, Fault Tolerance, vSAN, and others. You can also create VMkernel adapters on the source and target vSphere Replication hosts to isolate the replication data traffic.

Create a VMkernel Adapter on a vSphere Standard Switch on page 2195

Create a VMkernel network adapter on a vSphere standard switch to provide network connectivity for hosts and to handle the system traffic for vSphere vMotion, IP storage, Fault Tolerance logging, vSAN, and so on. You can also create VMkernel adapters on the source and target vSphere Replication hosts to isolate the replication data traffic. Dedicate a VMkernel adapter to only one traffic type.

Add a Virtual Machine Port Group on page 2151

Add VM port groups on a vSphere Standard Switch to provide connectivity and common network configuration for virtual machines.

Teaming and Failover Policy on page 2244

NIC teaming lets you increase the network capacity of a virtual switch by including two or more physical NICs in a team. To determine how the traffic is rerouted in case of adapter failure, you include physical NICs in a failover order. To determine how the virtual switch distributes the network traffic between the physical NICs in a team, you select load balancing algorithms depending on the needs and capabilities of your environment.

Port Group Configuration for Virtual Machines

You can add or modify a virtual machine port group to set up traffic management on a set of virtual machines.

The **Add Networking** wizard in the vSphere Client guides you through the process to create a virtual network to which virtual machines can connect, including creating a vSphere Standard Switch and configuring settings for a network label.

When you set up virtual machine networks, consider whether you want to migrate the virtual machines in the network between hosts. If so, ensure that the same broadcast domain is accessible by both hosts—that is, the same Layer 2 subnet.

does not support virtual machine migration between hosts in different broadcast domains because the migrated virtual machine might require systems and resources that it would no longer have access to in the new network. Even if your network configuration is set up as a high-availability environment or includes intelligent switches that can resolve the virtual machine's needs across different networks, you might experience lag times as the Address Resolution Protocol (ARP) table updates and resumes network traffic for the virtual machines.

Virtual machines reach physical networks through uplink adapters. A vSphere Standard Switch can transfer data to external networks only when one or more network adapters are attached to it. When two or more adapters are attached to a single standard switch, they are transparently teamed.

Add a Virtual Machine Port Group

Add VM port groups on a vSphere Standard Switch to provide connectivity and common network configuration for virtual machines.

1. In the vSphere Client, navigate to the host.
2. Right-click the host and select **Add Networking**.
3. In **Select connection type**, select **Virtual Machine Port Group for a Standard Switch** and click **Next**.
4. In **Select target device**, select an existing standard switch or create a new standard switch.
5. If the new port group is for an existing standard switch, navigate to the switch.
   a) Click **Browse**.
   b) Select a standard switch from the list and click **OK**.
   c) Click **Next** and go to Step 7.
6. Optional: If you choose to create a new standard switch, enter a value for the MTU size and click **Next**.

   You can create a standard switch with or without adapters.

   If you create a standard switch without physical network adapters, all traffic on that switch is confined to that switch. No other hosts on the physical network or virtual machines on other standard switches can send or receive traffic over this standard switch. You might create a standard switch without physical network adapters if you want a group of virtual machines to be able to communicate with each other, but not with other hosts or with virtual machines outside the group.

   a) Click **Add adapters**.
   b) Select an adapter from the **Network Adapters** list and click **OK**.
   c) Optional: Use the up and down arrows in the **Assigned adapters** list to change the position of the adapter if needed.
   d) Click **Next**.
7. On the Connection settings page, identify traffic through the ports of the group.
   a) Type a **Network label** for the port group, or accept the generated label.

      Note: Port group names must not contain a colon character (:).
   b) Set the **VLAN ID** to configure VLAN handling in the port group.

      The VLAN ID also reflects the VLAN tagging mode in the port group.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch passes traffic from any VLAN.

   c) Click **Next**.
8. Review the port group settings in the Ready to complete page, and click **Finish**.

   Click **Back** if you want to change any settings.

Related Links

VLAN Configuration on page 2281
Virtual LANs (VLANs) enable a single physical LAN segment to be further isolated so that groups of ports are isolated from one another as if they were on physically different segments.

Configure the Security Policy for a vSphere Standard Switch or Standard Port Group on page 2256
For a vSphere standard switch, you can configure the security policy to reject MAC address and promiscuous mode changes in the guest operating system of a virtual machine. You can override the security policy that is inherited from the standard switch on individual port groups.

Configure Traffic Shaping for a vSphere Standard Switch or Standard Port Group on page 2259
ESXi lets you shape outbound traffic on standard switches or port groups. The traffic shaper restricts the network bandwidth available to any port, but you can also configure it to temporarily allow bursts of traffic to flow through a port at higher speeds.

Configure NIC Teaming, Failover, and Load Balancing on a vSphere Standard Switch or Standard Port Group on page 2250
Include two or more physical NICs in a team to increase the network capacity of a vSphere Standard Switch or standard port group. Configure failover order to determine how network traffic is rerouted in case of adapter failure. Select a load balancing algorithm to determine how the standard switch distributes the traffic between the physical NICs in a team.

Create a vSphere Standard Switch on page 2149
Create a vSphere Standard Switch to provide network connectivity for hosts, virtual machines, and to handle VMkernel traffic. Depending on the connection type that you want to create, you can create a new vSphere Standard Switch with a VMkernel adapter, only connect physical network adapters to the new switch, or create the switch with a virtual machine port group.

Edit a Standard Switch Port Group

By using the vSphere Client, you can edit the name and VLAN ID of a standard switch port group, and override networking policies at the port group level.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select a standard switch from the list.
   The topology diagram of the switch appears.
4. In the topology diagram of the switch, click the name of the port group.
5. Next to the the topology diagram title, click the horizontal elipsis icon and select **Edit settings**.
6. On the Properties page, rename the port group in the **Network label** text field.
7. Configure VLAN tagging in the **VLAN ID** drop-down menu.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch passes traffic from any VLAN.

8. On the Security page, override the switch settings for protection against MAC address changes, forged transmits and for running virtual machines in promiscuous mode.
9. On the Traffic shaping page, override at the port group level the size of average and peak bandwidth and of bursts.
10. On the Teaming and failover page, override the teaming and failover settings inherited from the standard switch.

    You can configure traffic distribution and rerouting between the physical adapters associated with the port group. You can also change the order in which host physical adapters are used upon failure.
11. Click **OK**.

Related Links

VLAN Configuration on page 2281

Virtual LANs (VLANs) enable a single physical LAN segment to be further isolated so that groups of ports are isolated from one another as if they were on physically different segments.

Configure the Security Policy for a vSphere Standard Switch or Standard Port Group on page 2256

For a vSphere standard switch, you can configure the security policy to reject MAC address and promiscuous mode changes in the guest operating system of a virtual machine. You can override the security policy that is inherited from the standard switch on individual port groups.

Configure Traffic Shaping for a vSphere Standard Switch or Standard Port Group on page 2259

ESXi lets you shape outbound traffic on standard switches or port groups. The traffic shaper restricts the network bandwidth available to any port, but you can also configure it to temporarily allow bursts of traffic to flow through a port at higher speeds.

Configure NIC Teaming, Failover, and Load Balancing on a vSphere Standard Switch or Standard Port Group on page 2250

Include two or more physical NICs in a team to increase the network capacity of a vSphere Standard Switch or standard port group. Configure failover order to determine how network traffic is rerouted in case of adapter failure. Select a load balancing algorithm to determine how the standard switch distributes the traffic between the physical NICs in a team.

Remove a Port Group from a vSphere Standard Switch

You can remove port groups from vSphere Standard Switches in case you no longer need the associated labeled networks.

Verify that there are no powered-on virtual machines connected to the port group that you want to remove.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the standard switch.
4. From the topology diagram of the switch, select the port group that you want to remove by clicking its label.
5. From the toolbar in the switch topology, click the **Remove** action icon .

vSphere Standard Switch Properties

vSphere Standard Switch settings control switch-wide defaults for ports, which can be overridden by port group settings for each standard switch. You can edit standard switch properties, such as the uplink configuration and the number of available ports.

Number of Ports on ESXi Hosts

To ensure efficient use of host resources on ESXi hosts, the ports of virtual switches are dynamically scaled up and down. A switch on such a host can expand up to the maximum number of ports supported on the host. The port limit is determined based on the maximum number of virtual machines that the host can handle.

Change the Size of the MTU on a vSphere Standard Switch

Change the size of the maximum transmission unit (MTU) on a vSphere Standard Switch to improve the networking efficiency by increasing the amount of payload data transmitted with a single packet, that is, enabling jumbo frames.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select a standard switch from the table and click **Edit settings**.
4. Change the **MTU (Bytes)** value for the standard switch.

   You can enable jumbo frames by setting an MTU value greater than 1500. You cannot set an MTU size greater than 9000 bytes.
5. Click **OK**.

Change the Speed of a Physical Adapter

You can change the connection speed and duplex of a physical adapter to transfer data in compliance with the traffic rate.

If the physical adapter supports SR-IOV, you can enable it and configure the number of virtual functions to use for virtual machine networking.

1. In the vSphere Client, navigate to a host.
2. On the **Configure** tab, expand **Networking** and select **Physical adapters**.

   The physical network adapters of the host appear in a table that contains details for each physical network adapter.
3. Select the physical network adapter from the list and click the **Edit adapter settings** icon.
4. Select speed and duplex mode of the physical network adapter from the drop-down menu.

   The speed and duplex settings you select must match those configured on the physical switch. Speed is the rate of the interface, usually listed in megabits per second (Mbps). Duplex refers to how data flows on the interface.
5. Click **OK**.

Related Links

Enable SR-IOV on a Host Physical Adapter on page 2290

Before you can connect virtual machines to virtual functions, use the vSphere Client to enable SR-IOV and set the number of virtual functions on your host.

Add and Team Physical Adapters in a vSphere Standard Switch

Assign a physical adapter to a standard switch to provide connectivity to virtual machines and VMkernel adapters on the host. You can form a team of NICs to distribute traffic load and to configure failover.

NIC teaming combines multiple network connections to increase throughput and provide redundancy should a link fail. To create a team, you associate multiple physical adapters to a single vSphere Standard Switch.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the standard switch you want to add a physical adapter to.
4. Click **Manage Physical Adapters**.
5. Add one or more available physical network adapters to the switch.
   a) Click **Add adapters**, select one or more network adapters from the list and click **OK**.
      The selected adapters appear in the failover group list under the Assigned Adapters list.
   b) Optional: Use the up and down arrows to change the position of an adapter in the failover groups.
      The failover group determines the role of the adapter for exchanging data with the external network, that is, active, standby or unused. By default, the adapters are added as active to the standard switch.
6. Click **OK** to apply the physical adapter configuration.

View the Topology Diagram of a vSphere Standard Switch

You can examine the structure and components of a vSphere Standard Switch by using its topology diagram.

The topology diagram of a standard switch provides a visual representation of the adapters and port groups connected to the switch.

From the diagram you can edit the settings of a selected port group and of a selected adapter.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the standard switch from the list.

The diagram appears under the list of virtual switches on the host.

Diagram of a Standard Switch That Connects the VMkernel and Virtual Machines to the Network

In your virtual environment, a vSphere Standard Switch handles VMkernel adapters for vSphere vMotion and for the management network, and virtual machines grouped. You can use the central topology diagram to examine whether a virtual machine or VMkernel adapter is connected to the external network and to identify the physical adapter that carries the data.

Figure 50: Topology Diagram of a vSphere Standard Switch

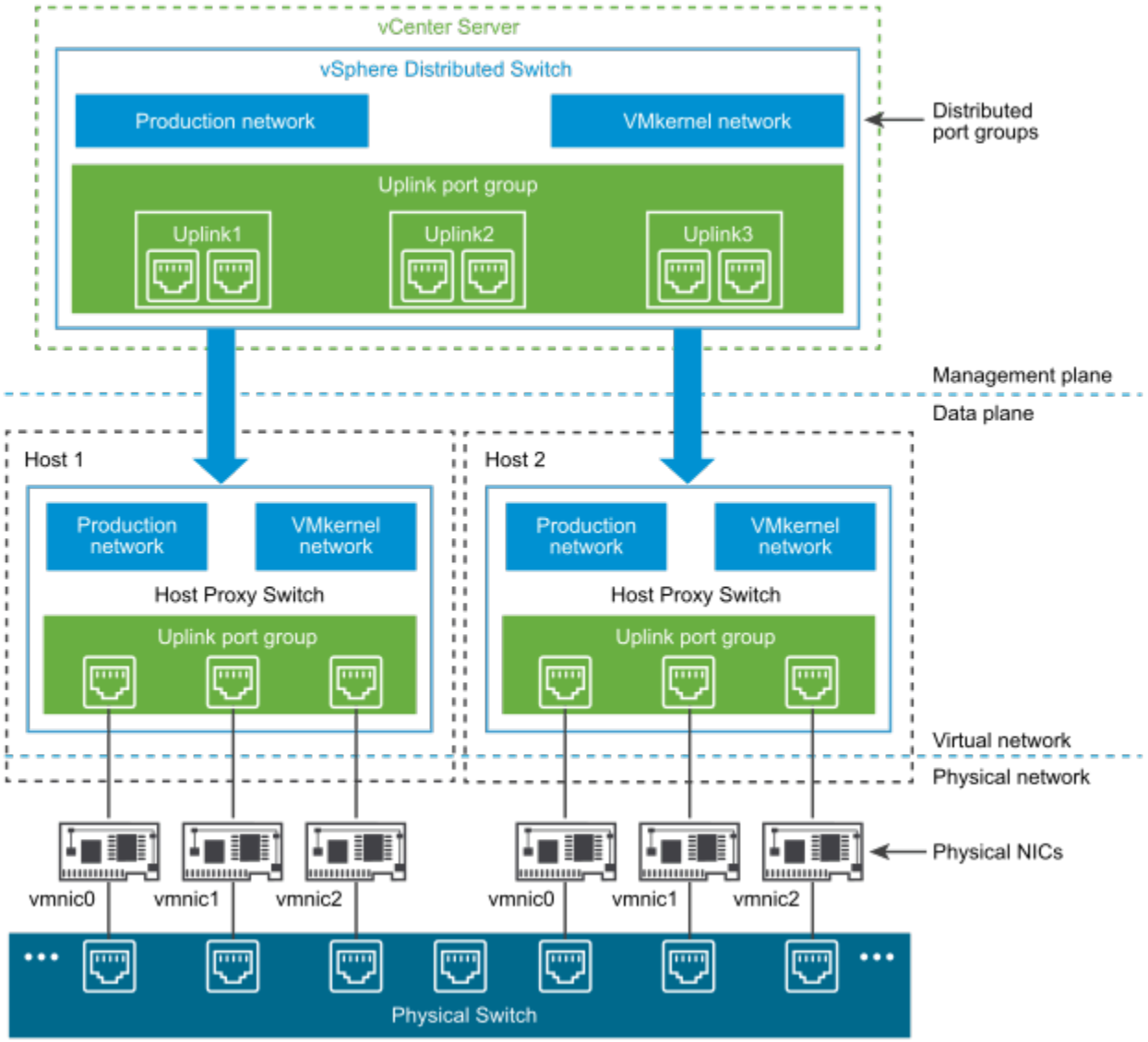
Setting Up Networking with vSphere Distributed Switches

With vSphere distributed switches you can set up and configure networking in a vSphere environment.

vSphere Distributed Switch Architecture

A vSphere Distributed Switch provides centralized management and monitoring of the networking configuration of all hosts that are associated with the switch. You set up a distributed switch on a vCenter Server system, and its settings are propagated to all hosts that are associated with the switch.

Figure 51: vSphere Distributed Switch Architecture



A network switch in vSphere consists of two logical sections that are the data plane and the management plane. The data plane implements the packet switching, filtering, tagging, and so on. The management plane is the control structure that you use to configure the data plane functionality. A vSphere Standard Switch contains both data and management planes, and you configure and maintain each standard switch individually.

A vSphere Distributed Switch separates the data plane and the management plane. The management functionality of the distributed switch resides on the vCenter Server system that lets you administer the networking configuration of your environment on a data center level. The data plane remains locally on every host that is associated with the distributed switch. The data plane section of the distributed switch is called a host proxy switch. The networking configuration that you create on vCenter Server (the management plane) is automatically pushed down to all host proxy switches (the data plane).

The vSphere Distributed Switch introduces two abstractions that you use to create consistent networking configuration for physical NICs, virtual machines, and VMkernel services.

Uplink port group	An uplink port group or dvuplink port group is defined during the creation of the distributed switch and can have one or

	more uplinks. An uplink is a template that you use to configure physical connections of hosts as well as failover and load balancing policies. You map physical NICs of hosts to uplinks on the distributed switch. At the host level, each physical NIC is connected to an uplink port with a particular ID. You set failover and load balancing policies over uplinks and the policies are automatically propagated to the host proxy switches, or the data plane. In this way you can apply consistent failover and load balancing configuration for the physical NICs of all hosts that are associated with the distributed switch.
Distributed port group	Distributed port groups provide network connectivity to virtual machines and accommodate VMkernel traffic. You identify each distributed port group by using a network label, which must be unique to the current data center. You configure NIC teaming, failover, load balancing, VLAN, security, traffic shaping , and other policies on distributed port groups. The virtual ports that are connected to a distributed port group share the same properties that are configured to the distributed port group. As with uplink port groups, the configuration that you set on distributed port groups on vCenter Server (the management plane) is automatically propagated to all hosts on the distributed switch through their host proxy switches (the data plane). In this way you can configure a group of virtual machines to share the same networking configuration by associating the virtual machines to the same distributed port group.

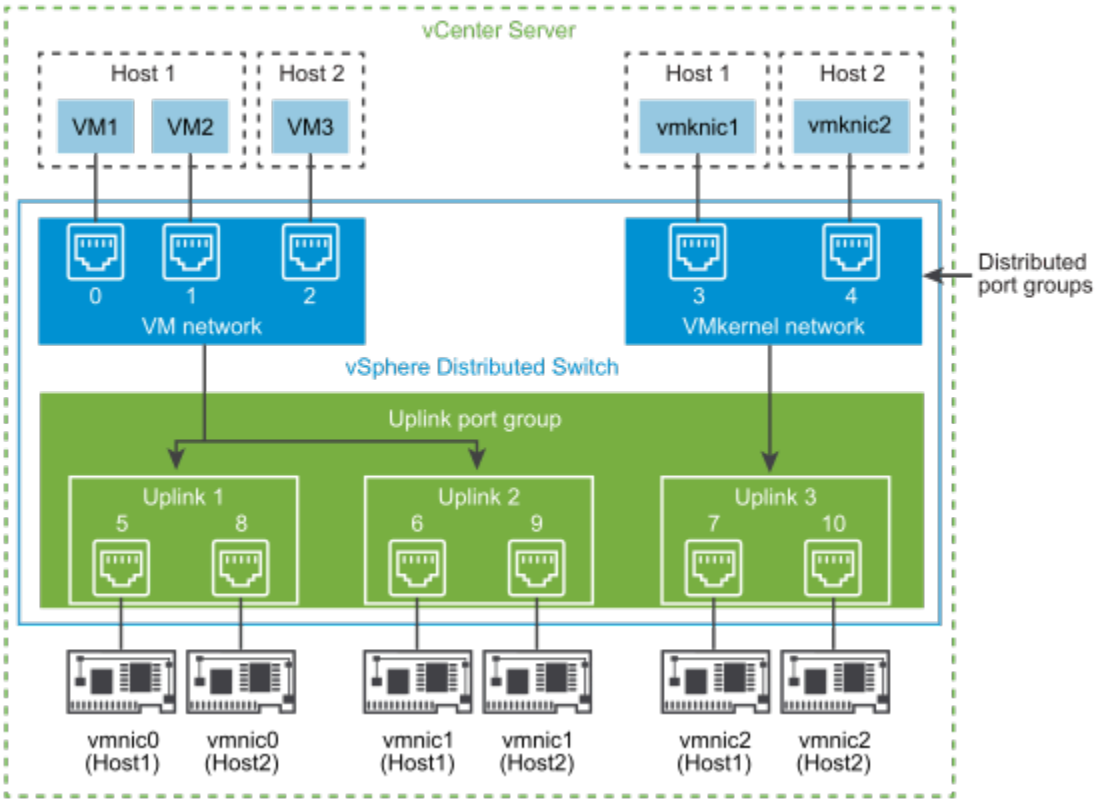
For example, suppose that you create a vSphere Distributed Switch on your data center and associate two hosts with it. You configure three uplinks to the uplink port group and connect a physical NIC from each host to an uplink. Each uplink has two physical NICs, one from each host which is mapped to it. For example, Uplink 1 is configured with vmnic0 from Host 1 and Host 2. Next you create the Production and the VMkernel network distributed port groups for virtual machine networking and VMkernel services. Respectively, a representation of the Production and the VMkernel network port groups is also created on Host 1 and Host 2. All policies that you set to the Production and the VMkernel network port groups are propagated to their representations on Host 1 and Host 2.

To ensure efficient use of host resources, the number of distributed ports of proxy switches is dynamically scaled up and down. A proxy switch on such a host can expand up to the maximum number of ports supported on the host. The port limit is determined based on the maximum number of virtual machines that the host can handle.

vSphere Distributed Switch Data Flow

The data flow from the virtual machines and VMkernel adapters down to the physical network depends on the NIC teaming and load balancing policies that are set to the distributed port groups. The data flow also depends on the port allocation on the distributed switch.

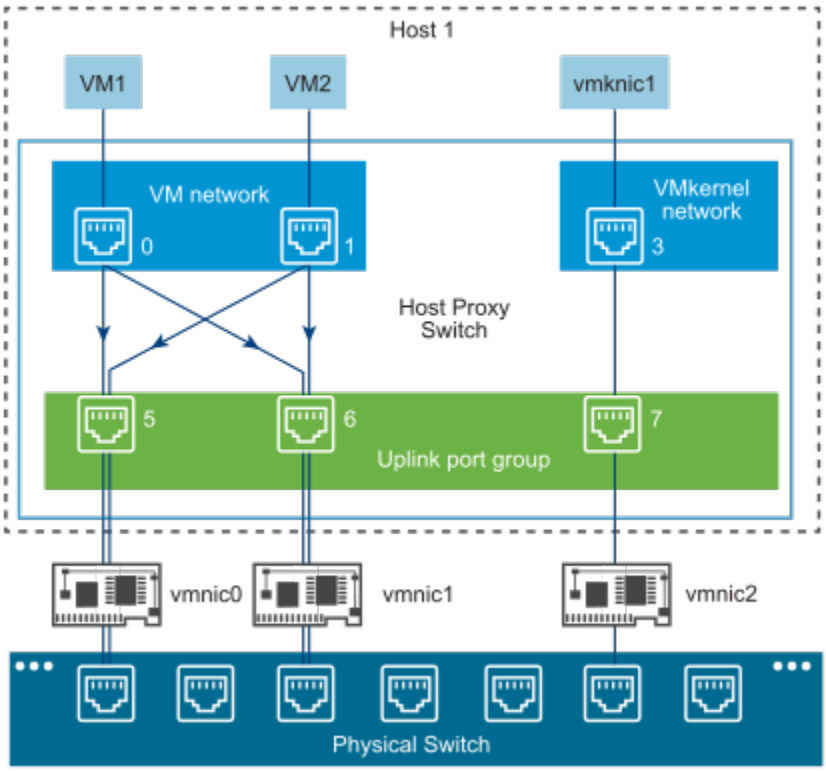
Figure 52: NIC Teaming and Port Allocation on a vSphere Distributed Switch



For example, suppose that you create the VM network and the VMkernel network distributed port groups, respectively with 3 and 2 distributed ports. The distributed switch allocates ports with IDs from 0 to 4 in the order that you create the distributed port groups. Next, you associate Host 1 and Host 2 with the distributed switch. The distributed switch allocates ports for every physical NIC on the hosts, as the numbering of the ports continues from 5 in the order that you add the hosts. To provide network connectivity on each host, you map vmnic0 to Uplink 1, vmnic1 to Uplink 2, and vmnic2 to Uplink 3.

To provide connectivity to virtual machines and to accommodate VMkernel traffic, you configure teaming and failover to the VM network and to the VMkernel network port groups. Uplink 1 and Uplink 2 handle the traffic for the VM network port group, and Uplink 3 handles the traffic for the VMkernel network port group.

Figure 53: Packet Flow on the Host Proxy Switch



On the host side, the packet flow from virtual machines and VMkernel services passes through particular ports to reach the physical network. For example, a packet sent from VM1 on Host 1 first reaches port 0 on the VM network distributed port group. Because Uplink 1 and Uplink 2 handle the traffic for the VM network port group, the packet can continue from uplink port 5 or uplink port 6 . If the packet goes through uplink port 5, it continues to vmnic0, and if the packet goes to uplink port 6, it continues to vmnic1.

Create a vSphere Distributed Switch

Create a vSphere distributed switch on a data center to handle the networking configuration of multiple hosts at a time from a central place.

1. In the vSphere Client, right-click a data center from the inventory tree.
2. Select **Distributed Switch** > **New Distributed Switch**.
3. On the Name and location page, enter a name for the new distributed switch, or accept the generated name, and click **Next.**
4. On the Select version page, select a distributed switch version and click **Next**.

Option	Description
Distributed Switch: 7.0.0	Compatible with ESXi 7.0 and later.
Distributed Switch: 6.6.0	Compatible with ESXi 6.7 and later. Features released with later vSphere distributed switch versions are not supported.
Distributed Switch: 6.5.0	Compatible with ESXi 6.5 and later. **Note:** Distributed Switch 6.5.0 is not compatible with ESXi 8.0 and later.

Option	Description
	Features released with later vSphere distributed switch versions are not supported.

5. On the Configure settings page, configure the distributed switch settings.
   a) Use the arrow buttons to select the **Number of uplinks**.

      Uplink ports connect the distributed switch to physical NICs on associated hosts. The number of uplink ports is the maximum number of allowed physical connections to the distributed switch per host.
   b) Use the drop-down menu to enable or disable **Network I/O Control**.

      By using Network I/O Control you can prioritize the access to network resources for certain types of infrastructure and workload traffic according to the requirements of your deployment. Network I/O Control continuously monitors the I/O load over the network and dynamically allocates available resources.
   c) Optional: Select the **Create a default port group** check box to create a new distributed port group with default settings for this switch. Enter a **Port group name**, or accept the generated name.

      If your system has custom port group requirements, create distributed port groups that meet those requirements after you add the distributed switch.
   d) Click **Next**.
6. On the Ready to complete page, review the settings you selected and click **Finish**.

   Use the **Back** button to edit any settings.

A distributed switch is created in the data center. You can view the features supported on the distributed switch as well as other details by navigating to the new distributed switch and clicking the **Summary** tab.

Add hosts to the distributed switch and configure their network adapters on the switch.

Related Links

Tasks for Managing Host Networking on a vSphere Distributed Switch on page 2164
You can add new hosts to a vSphere Distributed Switch, connect network adapters to the switch, and remove hosts from the switch. In a production environment, you might need to keep the network connectivity up for virtual machines and VMkernel services while you manage host networking on the distributed switch.

Add Hosts to a vSphere Distributed Switch on page 2165
To manage the networking of your vSphere environment by using a vSphere Distributed Switch, you must associate hosts with the switch. You connect the physical NICs, VMkernel adapters, and virtual machine network adapters of the hosts to the distributed switch.

Configure Physical Network Adapters on a vSphere Distributed Switch on page 2168
For hosts that are associated with a distributed switch, you can assign physical NICs to uplinks on the switch. You can configure physical NICs on the distributed switch for multiple hosts at a time.

Migrate VMkernel Adapters to a vSphere Distributed Switch on page 2169
Learn how to migrate VMkernel adapters to a distributed switch if you want to handle the traffic for VMkernel services by using only this switch when you no longer need the adapters on other standard or distributed switches.

Create a VMkernel Adapter on a vSphere Distributed Switch on page 2170
Create a VMkernel adapter on hosts associated with a distributed switch to provide network connectivity to the hosts and to handle the traffic for vSphere vMotion, IP storage, Fault Tolerance logging, and vSAN.

Migrate Virtual Machine Networking to the vSphere Distributed Switch on page 2179
To manage virtual machine networking by using a distributed switch, migrate virtual machine network adapters to labeled networks on the switch.

Use a Host as a Template to Create a Networking Configuration on a vDS

Upgrade a vSphere Distributed Switch to a Later Version

You can upgrade vSphere Distributed Switch version 6.x to a later version. The upgrade lets the distributed switch take advantage of features that are available only in the later version.

- Upgrade vCenter Server to version .
- Upgrade all hosts connected to the distributed switch to .

The upgrade of a distributed switch causes the hosts and virtual machines attached to the switch to experience a brief downtime.

Note: If your current vSphere Distributed Switch version is 6.5, then you might experience a brief interruption to network traffic, of a few milliseconds, while upgrading your vSphere Distributed Switch to a later version. For more information, see KB 52621. If your current vSphere Distributed Switch version is 6.6 or later there is no interruption to network traffic while upgrading your vSphere Distributed Switch to a later version.

Note:

To be able to restore the connectivity of the virtual machines and VMkernel adapters if the upgrade fails, back up the configuration of the distributed switch.

If the upgrade is not successful, to recreate the switch with its port groups and connected hosts, you can import the switch configuration file. See Export vSphere Distributed Switch Configurations and Import a vSphere Distributed Switch Configuration.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Upgrade** > **Upgrade Distributed Switch**.
3. Select the vSphere Distributed Switch version that you want to upgrade the switch to and click **Next**.

Option	Description
Distributed Switch: 7.0.3	Compatible with ESXi 7.0.3 and later. New Features and Enhancements • NVMe over TCP. See Create a VMkernel Adapter on a vSphere Standard Switch.
Distributed Switch: 7.0.2	Compatible with ESXi 7.0.2 and later. New Features and Enhancements • LACP Fast Mode. See LACP Support on a vSphere Distributed Switch.
Distributed Switch: 7.0.0	Compatible with ESXi 7.0 and later. New Features and Enhancements • NSX Distributed Port Group. See Networking Concepts Overview. **Note:** In vSphere 6.7, the default multicast filtering mode is Basic. In vSphere 7.0, the default multicast filtering mode is IGMP/MLD snooping. When the DVS is upgraded to 7.0, the default multicast filtering mode will change from basic to IGMP/MLD snooping.
Distributed Switch: 6.6.0	Compatible with ESXi 6.7 and later. Features released with later vSphere distributed switch versions are not supported. New Features and Enhancements • MAC Learning. See MAC Learning Policy

Option	Description
Distributed Switch: 6.5.0	Compatible with ESXi 6.5, ESXi 6.7, ESXi 7.0 and later versions. **Note:** Distributed Switch 6.5.0 is not compatible with ESXi 8.0.0 and later. New Features and Enhancements • Port Mirroring Enhancements. See Specify Port Mirroring Name and Session Details.

4. Review host compatibility and click **Next**.

   Some ESXi instances that are connected to the distributed switch might be incompatible with the selected target version. Upgrade or remove the incompatible hosts, or select another upgrade version for the distributed switch.

5. Complete the upgrade configuration and click **Finish**.

   CAUTION: After you upgrade the vSphere Distributed Switch, you cannot revert it to an earlier version. You also cannot add ESXi hosts that are running an earlier version than the new version of the switch.

Edit General and Advanced vSphere Distributed Switch Settings

General settings for a vSphere Distributed Switch include the switch name and number of uplinks. Advanced settings for a distributed switch include Cisco Discovery Protocol and the maximum MTU for the switch.

1. In the vSphere Client Home page, click **Networking** and select the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **Properties**.
3. Click **Edit**.
4. Click **General** to edit the vSphere Distributed Switch settings.

Option	Description
Name	Enter the name for the distributed switch.
Number of uplinks	Select the number of uplink ports for the distributed switch. Click **Edit uplink names** to change the names of the uplinks.
Network I/O Control	Use the drop-down menu to enable or disable Network I/O control.
Description	Add or modify a description of the distributed switch settings.

5. Click **Advanced** to edit the vSphere Distributed Switch settings.

Option	Description
MTU (Bytes)	Maximum MTU size for the vSphere Distributed Switch. To enable jumbo frames, set a value greater than 1500 bytes.
Multicast filtering mode	• **Basic**. The distributed switch forwards traffic that is related to a multicast group based on a MAC address generated from the last 23 bits of the IPv4 address of the group. • **IGMP/MLD snooping**. The distributed switch forwards multicast traffic to virtual machines according to the IPv4 and IPv6 addresses of subscribed multicast groups by using membership messages defined by the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery protocol.
Discovery Protocol	1. Select Cisco Discovery Protocol, Link Layer Discovery Protocol, or (disabled) from the **Type** drop-down menu. 2. Set **Operation** to Listen, Advertise, or Both.

Option	Description
	For information about Discovery Protocol, see Switch Discovery Protocol.
Administrator Contact	Enter the name and other details of the administrator for the distributed switch.

6. Click **OK**.

Managing Networking on Multiple Hosts on a vSphere Distributed Switch

You create and manage virtual networks on a vSphere Distributed Switch by adding hosts to the switch and connecting their network adapters to the switch. To create uniform networking configuration throughout multiple hosts on the distributed switch, you can use a host as a template and apply its configuration to other hosts.

Tasks for Managing Host Networking on a vSphere Distributed Switch

You can add new hosts to a vSphere Distributed Switch, connect network adapters to the switch, and remove hosts from the switch. In a production environment, you might need to keep the network connectivity up for virtual machines and VMkernel services while you manage host networking on the distributed switch.

Adding Hosts to a vSphere Distributed Switch

Consider preparing your environment before you add new hosts to a distributed switch.

- Create distributed port groups for virtual machine networking.
- Create distributed port groups for VMkernel services. For example, create distributed port groups for management network, vMotion, and Fault Tolerance.
- Configure enough uplinks on the distributed switch for all physical NICs that you want to connect to the switch. For example, if the hosts that you want to connect to the distributed switch have eight physical NICs each, configure eight uplinks on the distributed switch.
- Make sure that the configuration of the distributed switch is prepared for services with specific networking requirements. For example, iSCSI has specific requirements for the teaming and failover configuration of the distributed port group where you connect the iSCSI VMkernel adapter.

You can use the **Add and Manage Hosts** wizard in the to add multiple hosts at a time.

Managing Network Adapters on a vSphere Distributed Switch

After you add hosts to a distributed switch, you can connect physical NICs to uplinks on the switch, configure virtual machine network adapters, and manage VMkernel networking.

If some hosts on a distributed switch are associated to other switches in your data center, you can migrate network adapters to or from the distributed switch.

If you migrate virtual machine network adapters or VMkernel adapters, make sure that the destination distributed port groups have at least one active uplink, and the uplink is connected to a physical NIC on the hosts. Another approach is to migrate physical NICs, virtual network adapters, and VMkernel adapters simultaneously.

If you migrate physical NICs, leave at least one active NIC that handles the traffic of port groups. For example, if *vmnic0* and *vmnic1* handle the traffic of the *VM Network* port group, migrate *vmnic0* and leave *vmnic1* connected to the group.

Watch the video about migrating VMkernel interfaces and physical NICs to a vSphere Distributed Switch.

Removing Hosts from a vSphere Distributed Switch

Before you remove hosts from a distributed switch, you must migrate the network adapters that are in use to a different switch.

- To add hosts to a different distributed switch, you can use the **Add and Manage Hosts** wizard to migrate the network adapters on the hosts to the new switch all together. You can then remove the hosts safely from their current distributed switch.
- To migrate host networking to standard switches, you must migrate the network adapters in stages. For example, remove physical NICs on the hosts from the distributed switch by leaving one physical NIC on every host connected to the switch to keep the network connectivity up. Next, attach the physical NICs to the standard switches and migrate VMkernel adapters and virtual machine network adapters to the switches. Lastly, migrate the physical NIC that you left connected to the distributed switch to the standard switches.

Add Hosts to a vSphere Distributed Switch

To manage the networking of your vSphere environment by using a vSphere Distributed Switch, you must associate hosts with the switch. You connect the physical NICs, VMkernel adapters, and virtual machine network adapters of the hosts to the distributed switch.

- Verify that enough uplinks are available on the distributed switch to assign to the physical NICs that you want to connect to the switch.
- Verify that there is at least one distributed port group on the distributed switch.
- Verify that the distributed port group have active uplinks configured in its teaming and failover policy.

If you migrate or create VMkernel adapters for iSCSI, verify that the teaming and failover policy of the target distributed port group meets the requirements for iSCSI:

- Verify that only one uplink is active, the standby list is empty, and the rest of the uplinks are unused.

- Verify that only one physical NIC per host is assigned to the active uplink.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Add and Manage Hosts**.
3. On the Select task page, select **Add hosts**, and click **Next**.
4. On the Select hosts page,
   a) Select the host(s) from the list of available hosts under **All hosts**.
   b) To view the selected hosts, click **Selected**.
      The selected hosts are displayed.
   c) To filter the hosts based on their compatibility, click **Compatibility**.
   d) To select all the available hosts, click **Select All**.
5. Click **Next**.
6. On the **Manage physical adapters page**, you can add or remove network adapters to the distributed switch by assigning or unassigning an uplink.
7. To manage adapters on all hosts that have the same physical network adapter, select **Adapters on all hosts**.
   a) Click **Select All** to select all hosts.
   b) To assign an uplink to the host, select an uplink from the drop-down menu.
   c) To unassign an uplink from the hosts, select **None** from the drop-down menu.
   d) To see more details about the hosts, expand the network adapter listed under **Physical network adapters**.
   e) You can view the switches that use this VMkernel adapter in **In use by switch**.

   For instance, if you assign *uplink1* to *vmnic1*, it is assigned to all the hosts that have *vmnic1* as its physical network adapter.
8. To manager adapters per host, select **Adapters per host**.
   a) Select the individual host from the list.
   b) To assign an uplink to the host, select an uplink from the drop-down menu.
   c) To unassign an uplink from the host, select **None** from the drop-down menu.

   If you select physical NICs that are assigned to other standard or distributed switches, the NICs are migrated to the current distributed switch.

   For consistent network configuration, you can connect one and the same physical NIC on every host to the same uplink on the distributed switch.

   For instance, if you are adding two hosts connect *vmnic1* on each host to *Uplink1* on the distributed switch.
9. Click **Next**.

   Note: If a host does not have an assigned physical network adapter, then a warning appears.

10. On the **Manage VMkernel adapters page**, you can manage VMkernel adapters to the distributed switch.
11. To manage VMkernel adapters on all hosts that have the same VMkernel adapter, select **Adapters on all hosts**.
    a) To select all the hosts, click **Select All**.
    b) Click **Assign Port Group**.
       You can see all the available port groups.
    c) To assign a port group, click **Assign**.
    d) To unassign a port group, click **Unassign**.
    e) You can view the switches that use this VMkernel adapter in **In use by switch**.
    f) To see more details about the hosts, expand the VMkernel adapter listed under **Name**.

    For instance, if you assign *DPortGroup1* to *vmk0*, the port group is assigned to all the hosts that has *vmk0* as its VMkernel network adapter.
12. To manage VMkernel adapter per host, select **Adapters per host**.
    a) Select the individual host from the list.
    b) Click **Assign Port Group**.
       You can see all the available port groups.
    c) To assign a port group, click **Assign**.
    d) To unassign a port group, click **Unassign**.
13. Click **Next**.
14. On the **Migrate VM networking** page, select the check box **Migrate virtual machine networking** to migrate virtual machines to a distributed switch.
15. To configure per network adapter, click **Assign port group**.
    a) To assign a port group, click **Assign**.
       For instance, the port group is assigned to all the virtual machines that have the same network adapter.
    b) To unassign port groups, click **Unassign**.
16. To configure per virtual machine, click **Assign port group**.
    a) To assign a port group, click **Assign**.
    b) To unassign a port group, click **Unassign**.
17. Click **Next**.
18. On the **Ready to Complete** page of the **Add and Manage Hosts** wizard, review the settings for the virtual machine.
19. Click **Finish**.
    You have now successfully added a host to the vSphere distributed switch.

Having hosts associated with the distributed switch, you can manage physical network adapters, VMkernel adapters, and virtual machine network adapters.

Configure Physical Network Adapters on a vSphere Distributed Switch

For hosts that are associated with a distributed switch, you can assign physical NICs to uplinks on the switch. You can configure physical NICs on the distributed switch for multiple hosts at a time.

For consistent networking configuration throughout all hosts, you can assign the same physical NIC on every host to the same uplink on the distributed switch. For example, you can assign *vmnic1* from hosts *ESXi A* and *ESXi B* to *Uplink 1*.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Add and Manage Hosts**.
3. On the Select task page, select **Manage host networking** and click **Next**.
4. On the Select hosts page, under **Member Hosts**, select from the hosts that are associated with the distributed switch.
5. Click **Next**.
6. On the **Manage physical adapters page**, you can add or remove network adapters to the distributed switch by assigning or unassigning an uplink.
7. To manage adapters on all hosts that have the same physical network adapter, select **Adapters on all hosts**.

   The user can see `--` while selecting an option in the uplinks drop down menu. This option indicates that not all the hosts with the same network adapter can be assigned to the same uplink.

   For example, if *vmnic 0* is assigned to *Uplink 1* in *ESXI A*, and to *Uplink 2* in *ESXI B* then the `--` option will be selected in the drop down menu. Selecting this option and moving to the next operation does not change any configuration.

   a) To assign an uplink to the host, select an uplink from the drop-down menu.
   b) To unassign an uplink from the hosts, select **None** from the drop-down menu
   c) You can view the switches that use this VMkernel adapter in **In use by switch**.
   d) To see more details about the hosts, expand the network adapter listed under **Physical network adapters**.
8. To manage adapters per host, select **Adapters per host**.
   a) Select the individual host from the list.
   b) To assign an uplink to the host, select an uplink from the drop-down menu.
   c) To unassign an uplink from the host, select **None** from the drop-down menu.

   Note: While adding hosts to the vSphere Distributed Switch with network offloads compatibility, you can only add a compatible adapter that is supported by a compatible DPU.

   If you select physical NICs that are already assigned to other standard or distributed switches, the NICs are migrated to the current distributed switch.

   For consistent network configuration, you can connect one and the same physical NIC on every host to the same uplink on the distributed switch.

   For example, if you are adding two hosts connect *vmnic1* on each host to *Uplink1* on the distributed switch.
9. Click **Next**.

   Note: If a host does not have an assigned physical network adapter, then a warning appears.

10. On the **Manage VMkernel adapters** page, you can add VMkernel adapters to the distributed switch.
11. On the **Migrate VM networking** page, select the check box **Migrate virtual machine networking** to migrate virtual machines to a distributed switch.
12. Click **Next**.
13. On the **Ready to Complete** page of the **Add and Manage Hosts** wizard, review the settings for the virtual machine.
14. Click **Finish**.

Migrate VMkernel Adapters to a vSphere Distributed Switch

Learn how to migrate VMkernel adapters to a distributed switch if you want to handle the traffic for VMkernel services by using only this switch when you no longer need the adapters on other standard or distributed switches.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Add and Manage Hosts**.
3. On the Select task page, select **Manage host networking** and click **Next**.
4. On the Select hosts page, under **Member Hosts**, select from the hosts that are associated with the distributed switch.
5. Click **Next**.
6. On the **Manage physical adapters page**, you can add or remove network adapters to the distributed switch by assigning or unassigning an uplink.
7. Click **Next**.

   Note: If a host does not have an assigned physical network adapter, then a warning appears.
8. On the **Manage VMkernel adapters page**, you can manage VMkernel adapters to the distributed switch.
9. To manage VMkernel adapters on all hosts that have the same VMkernel adapter, select **Adapters on all hosts**.
   a) Click **Assign Port Group**

      You can see all the available port groups.
   b) To assign a port group, click **Assign**.
   c) To unassign a port group, click **Unassign**.

   For instance, if you assign *DPortGroup1* to *vmk0*, the port group is assigned to all the hosts that has *vmk0* as its VMkernel network adapter.

10. To see more details about the hosts, expand the VMkernel adapter listed under **Name**.
11. You can view the switches that use this VMkernel adapter in **In use by switch**.
12. To manager VMkernel adapter per host, select **Adapters per host**.
    a) Select the individual host from the list.
    b) Click **Assign Port Group**.
       You can see all the available port groups.
    c) To assign a port group, click **Assign** .
    d) To unassign a port group, click **Unassign**.
13. Click **Next**.
14. On the **Migrate VM networking** page, select the check box **Migrate virtual machine networking** to migrate virtual machines to a distributed switch.
15. Click **Next**.
16. On the **Ready to Complete** page of the **Add and Manage Hosts** wizard, review the settings for the virtual machine.
17. Click **Finish**.

Create a VMkernel Adapter on a vSphere Distributed Switch

Create a VMkernel adapter on hosts associated with a distributed switch to provide network connectivity to the hosts and to handle the traffic for vSphere vMotion, IP storage, Fault Tolerance logging, and vSAN.

You should dedicate one distributed port group for each VMkernel adapter. One VMkernel adapter should handle only one traffic type.

1. On the vSphere Client Home page, click **Networking** and navigate to a distributed port group.
2. From the **Actions** menu, select **Add VMkernel Adapters**.
3. On the Select hosts page, click **Attached hosts**, select from the hosts that are associated with the distributed switch and click **OK**.
4. Click **Next**.
5. On the Configure VMkernel adapter page, configure the settings for the VMkernel adapter.

Option	Description
Network label	The network label is inherited from the label of the distributed port group.
IP settings	Select IPv4, IPv6, or both.

Option	Description
	Note: The IPv6 option does not appear on hosts that do not have IPv6 enabled.
MTU	Choose whether to get MTU for the network adapter from the switch or to set a custom size. You cannot set the MTU size to a value greater than 9000 bytes.
TCP/IP stack	Select a TCP/IP stack from

Option	Description
	the list. Once you set a TCP/IP stack for the VMkernel adapter, you cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you will be able to use only these stacks to handle vMotion or Provisioning traffic on the host. All VMkernel adapters for vMotion

Option	Description
	on the default TCP/IP stack are deactivated for future vMotion sessions. If you set the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are deactivated for operations that include Provisioning traffic, such as virtual machine cold migration, cloning, and snapshot migration.
Available services	You can enable services for the

Option	Description
	default TCP/IP stack on the host. Select from the available services: • **vMotion**. Enables the VMkerne adapter to advertise itself to another host as the network connectio where vMotion traffic is sent. The migration with vMotion to the selected host is not possible if the vMotion service is not enabled for any VMkerne adapter on the default

Option	Description
	TCP/IP stack, or there are no adapters using the vMotion TCP/IP stack. • **Provisio** Handles the data transferre for virtual machine cold migration cloning, and snapshot migration • **Fault Toleranc logging**. Enables Fault Tolerance logging on the host. You can use only one VMkerne adapter for FT traffic per host. • **Manager** Enables the managem traffic for the

Option	Description
	host and vCenter Server. Typically, hosts have such a VMkerne adapter created when the ESXi software is installed. You can create another VMkerne adapter for managen traffic on the host to provide redundar • **vSphere Replicati** Handles the outgoing replicatio data that is sent from the source ESXi host to the vSphere Replicati server. • **vSphere Replicati NFC**. Handles

Option	Description
	the incoming replicatio data on the target replicatio site. • **vSAN**. Enables the vSAN traffic on the host. Every host that is part of a vSAN cluster must have such a VMkerne adapter. • **vSphere Backup NFC**. VMkerne port setting for dedicate backup NFC traffic. NFC traffic goes through the VMkerne Adapter when vSphereE NFC service is enabled.

Option	Description
	• **NVMe over TCP**. VMkerne port setting for dedicated NVMe over TCP storage traffic. NVMe over TCP storage traffic goes through the VMkerne Adapter when NVMe over TCP adapter is enabled. For more informati see *vSphere Storage Guide*. • **NVMe over RDMA**. VMkerne port setting for dedicated NVMe over RDMA storage traffic. NVMe over RDMA storage traffic goes through

Option	Description
	the VMkerne Adapter when NVMe over RDMA adapter is enabled. For more informati see *vSphere Storage Guide*.

6. On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack. To change the VMkernel default gateway, select **Configure on VMkernel adapters** or **Configure on TCP/IP stack and enter a gateway address**.

7. On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisement to obtain IPv6 addresses. In ESXi 6.5 and later router advertisement is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	1. Enter the IPv6 address and subnet prefix length. 2. To change the VMkernel default gateway, select **Configure on VMkernel adapters** or **Configure on TCP/IP stack and enter a gateway address**. The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

8. Review your settings selections on the Ready to complete page and click **Finish**.

Migrate Virtual Machine Networking to the vSphere Distributed Switch

To manage virtual machine networking by using a distributed switch, migrate virtual machine network adapters to labeled networks on the switch.

Verify that at least one distributed port group intended for virtual machine networking exists on the distributed switch.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the Select task page, select **Manage host networking** and click **Next**.
3. On the Select hosts page, under **Member Hosts**, select from the hosts that are associated with the distributed switch.
4. Click **Next**.
5. On the **Manage physical adapters page**, you can add or remove network adapters to the distributed switch by assigning or unassigning an uplink.
6. Click **Next**.

   Note: If a host does not have an assigned physical network adapter, then a warning appears.
7. On the **Manage VMkernel adapters page**, you can add VMkernel adapters to the distributed switch.
8. On the **Migrate VM networking** page, select the check box **Migrate virtual machine networking** to migrate virtual machines to a distributed switch.
9. To configure per network adapter, click **Assign port group**.
   a) To assign a port group, click **Assign**.
      For instance, the port group is assigned to all the virtual machines that have the same network adapter.
   b) To unassign a port group, click **Unassign**.
10. To configure per virtual machine, click **Assign port group**.
    a) To assign a port group, click **Assign**.
    b) To unassign a port group, click **Unassign**.
11. Click **Next**.
12. On the **Ready to Complete** page of the **Add and Manage Hosts** wizard, review the settings for the virtual machine.
13. Click **Finish**.

Remove Hosts from a vSphere Distributed Switch

Remove hosts from a vSphere distributed switch if you have configured a different switch for the hosts.

- Verify that physical NICs on the target hosts are migrated to a different switch.
- Verify that VMkernel adapters on the hosts are migrated to a different switch.
- Verify that virtual machine network adapters are migrated to a different switch.

For details about migrating network adapters to different switches, see Tasks for Managing Host Networking on a vSphere Distributed Switch

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. From the **Actions** menu, select **Add and Manage Hosts**.
3. On the Select task page, select **Remove hosts** and click **Next**.
4. To remove an individual host from the distributed switch, select the host.
5. To remove all the hosts from the distributed switch, click **Select All**.
6. Click **Next**.
7. Click **Finish**.

Managing Networking on Host Proxy Switches

You can change the configuration of the proxy switch on every host that is associated with a vSphere distributed switch. You can manage physical NICs, VMkernel adapters, and virtual machine network adapters.

For details about setting up VMkernel networking on host proxy switches, see Create a VMkernel Adapter on a vSphere Distributed Switch.

Migrate Network Adapters on a Host to a vSphere Distributed Switch

For hosts associated with a distributed switch, you can migrate network adapters from a standard switch to the distributed switch. You can migrate physical NICs, VMkernel adapters, and virtual machine network adapters at the same time.

To migrate virtual machine network adapters or VMkernel adapters, make sure that the destination distributed port groups have at least one active uplink, and the uplink is connected to a physical NIC on this host. Alternatively, migrate physical NICs, virtual network adapters, and VMkernel adapters at once.

To migrate physical NICs, make sure that the source port groups on the standard switch have at least one physical NIC to handle their traffic. For example, if you migrate a physical NIC that is assigned to a port group for virtual machine

networking, make sure that the port group is connected to at least one physical NIC. Otherwise the virtual machines on same VLAN on the standard switch will have connectivity between each other but not to the external network.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the destination distributed switch and click the horizontal elipsis icon next to **Manage physical adapters**.
4. Select **Migrate Networking**..
5. Configure physical NICs.
   a) From the **On other switches/unclaimed** list, select a physical NIC and click **Assign uplink**.
   b) Select an uplink and click **OK**.
   c) Click **Next**.
6. Configure VMkernel adapters.
   a) Select an adapter and click **Assign port group**.
   b) Select a distributed port group and click **OK**.
      You should connect one VMkernel adapter to one distributed port group at a time.
   c) Click **Next**.
7. Configure virtual machine network adapters.
   a) Select the check box **Migrate virtual machine networking**.
   b) Select a virtual machine or a virtual machine network adapter and click **Assign port group**.
      If you select a virtual machine, you migrate all network adapters on the virtual machine. If you select a network adapter, you migrate only this network adapter.
   c) Select a distributed port group from the list and click **OK**.
   d) Click **Next**.
8. On the Ready to complete page, review the new networking configuration and click **Finish**.

Migrate a VMkernel Adapter on a Host to a vSphere Standard Switch

If a host is associated with a distributed switch, you can migrate VMkernel adapters from the distributed to a standard switch.

Verify that the destination standard switch has at least one physical NIC.

For details about creating VMkernel adapters on a vSphere distributed switch, see Create a VMkernel Adapter on a vSphere Distributed Switch.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the destination standard switch from the list.
4. Click **Migrate VMkernel Adapter**.
5. On the Select VMkernel adapter page, select the virtual network adapter to migrate to the standard switch from the list.
6. On the Configure settings page, edit the **Network label** and **VLAN ID** for the network adapter.
7. On the Ready to complete page, review the migration details and click **Finish**.
   Click **Back** to edit settings.

Assign a Physical NIC of a Host to a vSphere Distributed Switch

You can assign physical NICs of a host that is associated with a distributed switch to uplink port on the host proxy switch.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select a distributed switch from the list.
4. Click **Manage Physical Adapters**.
5. Select a free uplink from the list and click **Add adapters**.
6. Select a physical NIC and click **OK**.

Remove a Physical NIC from a vSphere Distributed Switch

You can remove a physical NIC of a host from an uplink on a vSphere distributed switch.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the distributed switch.
4. Click **Manage Physical Adapters**.
5. Select an uplink an click **Remove selected**.
6. Click **OK**.

When you remove physical NICs from active virtual machines, you might see the NICs you removed reported in the . See Removing NICs from Active Virtual Machines.

Removing NICs from Active Virtual Machines

When you remove NICs from active virtual machines, you can see the NICs you have removed in the vSphere Client.

Removing NICs from an Active Virtual Machine without a Guest Operating System Installed

You cannot remove NICs from an active virtual machine on which no operating system is installed.

The vSphere Client might report that the NIC has been removed, but you continue to see it attached to the virtual machine.

Removing NICs from an Active Virtual Machine with a Guest Operating System Installed

You can remove a NIC from an active virtual machine, but it might not be reported to the vSphere Client for some time. If you click **Edit Settings** for the virtual machine, you might see the removed NIC listed even after the task is complete. The Edit Settings dialog box for the virtual machine does not immediately display the removed NIC.

You might also see the NIC attached to the virtual machine if the guest operating system of the virtual machine does not support hot removal of NICs.

Distributed Port Groups

A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

Add a Distributed Port Group

To create a distributed switch network for your virtual machines, and to associate VMkernel adapters, you can add a distributed port group to a vSphere Distributed Switch.

Related to adding a port group, is applying VLAN tagging globally on all distributed ports. Using the VLAN options you can select VLAN tags. To learn more, see Configure VLAN Tagging on a Distributed Port Group or Distributed Port.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Distributed port group** > **New distributed port group**.
3. On the Name and location page, enter the name of the new distributed port group, or accept the generated name, and click **Next**.
4. On the Configure settings page, set the general properties for the new distributed port group and click **Next**.

Setting	Description
Port binding	Select when ports are assigned to virtual machines connected to this distributed port group. • **Static binding**: Assign a port to a virtual machine when the virtual machine connects to the distributed port group. • **Ephemeral - no binding**: No port binding. You can assign a virtual machine to a distributed port group with ephemeral port binding also when connected to the host.
Port allocation	• **Elastic:** The default number of ports is eight. When all ports are assigned, a new set of eight ports is created. • **Fixed**: The default number of ports is set to eight. No additional ports are created when all ports are assigned.
Number of ports	Enter the number of ports on the distributed port group.
Network resource pool	Use the drop-down menu to assign the new distributed port group to a user-defined network resource pool. If you have not created a network resource pool, this menu is empty.
VLAN	Use the **VLAN type** drop-down menu to specify the type of VLAN traffic filtering and marking: • **None**: Do not use VLAN. Select this option if you are using External Switch Tagging. • **VLAN**: In the **VLAN ID** text box, enter a number between 1 and 4094 for Virtual Switch Tagging. • **VLAN trunking**: Enter a VLAN trunk range. Pass VLAN traffic with an ID to the guest OS. You can set multiple ranges and individual VLANs by using a comma-separated list. For example: `1702-1705, 1848-1849` Use this option for Virtual Guest Tagging. • **Private VLAN**: Associate the traffic with a private VLAN created on the distributed switch. If you did not create any private VLANs, this menu is empty.
Advanced	To customize the policy configurations for the new distributed port group, select this check box.

5. Optional: On the Security page, edit the security exceptions and click **Next**.

Setting	Description
Promiscuous mode	• **Reject**. Placing an adapter in promiscuous mode from the guest operating system does not result in receiving frames for other virtual machines.

Setting	Description
	• **Accept**. If an adapter is placed in promiscuous mode from the guest operating system, the switch allows the guest adapter to receive all frames passed on the switch in compliance with the active VLAN policy for the port where the adapter is connected. • Firewalls, port scanners, intrusion detection systems, and so on, must run in promiscuous mode.
MAC address changes	• **Reject**. If you set this option to **Reject** and the guest OS changes the MAC address of the adapter to a value different from the address in the `.vmx` configuration file, the switch drops all inbound frames to the virtual machine adapter. • If the guest OS changes the MAC address back, the virtual machine receives frames again. • **Accept**. If the guest OS changes the MAC address of a network adapter, the adapter receives frames to its new address.
Forged transmits	• **Reject**. The switch drops any outbound frame with a source MAC address that is different from the one in the `.vmx` configuration file. • **Accept**. The switch does not perform filtering and permits all outbound frames.

6. Optional: On the Traffic shaping page, enable or disable Ingress or Egress traffic shaping and click **Next**.

Setting	Description
Status	If you enable either **Ingress traffic shaping** or **Egress traffic shaping**, you are setting limits on the amount of networking bandwidth allocated for each virtual adapter associated with this particular port group. If you disable the policy, services have a free, clear connection to the physical network by default.
Average bandwidth	Establishes the number of bits per second to allow across a port, averaged over time. This is the allowed average load.
Peak bandwidth	The maximum number of bits per second to allow across a port when it is sending and receiving a burst of traffic. This tops the bandwidth used by a port whenever it is using its burst bonus.
Burst size	The maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by **Average bandwidth**, it might temporarily transmit data at a faster speed if a burst bonus is available. This parameter tops the number of bytes that might be accumulated in the burst bonus and as a result transferred at a faster speed.

7. Optional: On the Teaming and failover page, edit the settings and click **Next**.

Setting	Description
Load balancing	Specify how to choose an uplink. • **Route based on originating virtual port**. Choose an uplink based on the virtual port where the traffic entered the distributed switch. • **Route based on IP hash**. Choose an uplink based on a hash of the source and destination IP addresses of each

Setting	Description
	packet. For non-IP packets, whatever is at those offsets is used to compute the hash. • **Route based on source MAC hash**. Choose an uplink based on a hash of the source Ethernet. • **Route based on physical NIC load**. Choose an uplink based on the current loads of physical NICs. • **Use explicit failover order**. Always use the highest order uplink from the list of Active adapters which passes failover detection criteria. **Note:** IP-based teaming requires that the physical switch is configured with EtherChannel. For all other options, disable EtherChannel.
Network failure detection	Specify the method to use for failover detection. • **Link status only**. Relies solely on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch. • **Beacon probing**. Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. This detects many of the failures previously mentioned that are not detected by link status alone. **Note:** Do not use beacon probing with IP-hash load-balancing.
Notify switches	Select **Yes** or **No** to notify switches in case of failover. If you select **Yes**, whenever a virtual NIC is connected to the distributed switch or whenever that virtual NIC's traffic might be routed over a different physical NIC in the team because of a failover event, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this process is desirable for the lowest latency of failover occurrences and migrations with vMotion. If the **Notify switches** is set to **Yes**, then all the connected ports, port groups, and distributed switches are connected back to the host when vCenter Server reconnects with ESXi hosts. **Note:** Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode.
Failback	Select **Yes** or **No** to disable or enable failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. If failback is set to **Yes** (default), the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. If failback is set to **No**, a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.

Setting	Description
Failover order	Specify how to distribute the workload for uplinks. To use some uplinks but reserve others for emergencies if the uplinks in use fail, set this condition by moving them into different groups: • **Active uplinks**. Continue to use the uplink when the network adapter connectivity is up and active. • **Standby uplinks** . Use this uplink if one of the active adapters' connectivity is down. • **Unused uplinks** . Do not use this uplink. **Note:** When using IP-hash load-balancing, do not configure standby uplinks.

8. Optional: On the Monitoring page, enable or disable NetFlow and click **Next**.

Setting	Description
Disabled	NetFlow is disabled on the distributed port group.
Enabled	NetFlow is enabled on the distributed port group. NetFlow settings can be configured at the vSphere Distributed Switch level.

9. Optional: On the Miscellaneous page, select **Yes** or **No** and click **Next**.

   Selecting **Yes** shuts down all ports in the port group. This action might disrupt the normal network operations of the hosts or virtual machines using the ports.

10. On the Ready to complete page, review your settings and click **Finish**.

    To change any settings, click the **Back** button.

Edit General Distributed Port Group Settings

You can edit general distributed port group settings such as the distributed port group name, port settings and network resource pool.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Right-click the distributed port group and select **Edit Settings**.
3. Select **General** to edit the following distributed port group settings.

Option	Description
Name	The name of distributed port group. You can edit the name in the text field.
Port binding	Choose when ports are assigned to virtual machines connected to this distributed port group. • **Static binding**: Assign a port to a virtual machine when the virtual machine connects to the distributed port group. • **Ephemeral**: No port binding. You can also assign a virtual machine to a distributed port group with ephemeral port binding when connected to the host.
Port allocation	• **Elastic:** The default number of ports is set to eight. When all ports are assigned, a new set of eight ports is created. This is the default.

Option	Description
	• **Fixed**: The default number of ports is set to eight. No additional ports are created when all ports are assigned.
Number of ports	Enter the number of ports on the distributed port group.
Network resource pool	Use the drop-down menu to assign the new distributed port group to a user-defined network resource pool. If you have not created a network resource pool, this menu is empty.
Description	Enter any information about the distributed port group in the description field.

4. Click **OK**.

Remove a Distributed Port Group

Remove a distributed port group when you no longer need the corresponding labeled network to provide connectivity and configure connection settings for virtual machines or VMkernel networking.

- Verify that all virtual machines connected to the corresponding labeled network are migrated to a different labeled network.
- Verify that all VMkernel adapters connected to the distributed port group are migrated to a different port group, or are deleted.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Select the distributed port group.
3. From the **Actions** menu, select **Delete**.

Working with Distributed Ports

A distributed port is a port on a vSphere distributed switch that connects to the VMkernel or to a virtual machine's network adapter.

Default distributed port configuration is determined by the distributed port group settings, but some settings for individual distributed ports can be overridden.

Monitor the State of Distributed Ports

vSphere can monitor distributed ports and provide information about the current state and runtime statistics of each port.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Click a distributed port group.
3. Click the **Ports** tab and select a port from the list.

   The ports table for the distributed port group displays runtime statistics for each distributed port.

   The **State** column displays the current state for each distributed port.

Option	Description
Link Up	The link for this distributed port is up.
Link Down	The link for this distributed port is down.

Option	Description
Blocked	This distributed port is blocked.
--	The state of this distributed port is currently unavailable.

Configure Distributed Port Settings

You can change general distributed port settings such as the port name and description.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Click a distributed port group from the list.
3. Click the **Ports** tab, and select a distributed port from the table.
   Information about the distributed port appears at the bottom of the screen.
4. Click the **Edit settings** icon.
5. On the Properties page and policy pages, edit information about the distributed port and click **OK**.

   If overrides are not allowed, the policy options are disabled.

   You can allow overrides at the port level by changing the **Advanced** settings of the distributed port group. See Configure Overriding Networking Policies on Port Level.

Configuring Virtual Machine Networking on a vSphere Distributed Switch

Connect virtual machines to a vSphere distributed switch either by configuring an individual virtual machine NIC or migrating groups of virtual machines from the vSphere distributed switch itself.

Connect virtual machines to vSphere distributed switches by connecting their associated virtual network adapters to distributed port groups. You can do this either for an individual virtual machine by modifying the virtual machine's network adapter configuration, or for a group of virtual machines by migrating virtual machines from an existing virtual network to a vSphere distributed switch.

Migrate Virtual Machines to or from a vSphere Distributed Switch

In addition to connecting virtual machines to a distributed switch at the individual virtual machine level, you can migrate a group of virtual machines between a vSphere Distributed Switch network and a vSphere Standard Switch network.

1. In the vSphere Client, navigate to a data center.
2. Right-click the data center in the navigator and select **Migrate VMs to Another Network**.
3. Select a source network.
   - Select **Specific network** and use the **Browse** button to select a specific source network.
   - Select **No network** to migrate all virtual machine network adapters that are not connected to any other network.
4. Use **Browse** to select a destination network and click **Next**.
5. Select virtual machines from the list to migrate from the source network to the destination network and click **Next**.
6. Review your selections and click **Finish**.
   Click **Back** to edit any selections.

Connect an Individual Virtual Machine to a Distributed Port Group

Connect an individual virtual machine to a vSphere Distributed Switch by modifying the NIC configuration of the virtual machine.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. From the Actions menu, select Edit Settings.
3. Expand the **Network adapter** section and select **Browse** from the **Network adapter** drop-down menu.
4. In the Select Network dialog box, select a distributed port group and click **OK**.
5. Click **OK**.

Topology Diagrams of a vSphere Distributed Switch

The topology diagrams of a vSphere Distributed Switch in the vSphere Client show the structure of virtual machine adapters, VMkernel adapters, and physical adapters in the switch.

You can examine the components, arranged in port groups, whose traffic is handled by the switch, and the connections between them. The diagram displays information about the physical adapter that connects the virtual adapters to the external network.

You can view the components that are running on the entire distributed switch and on each host participating in it.

Watch the video about the operations that you can perform from the topology diagram of vSphere Distributed Switch.

Central Topology Diagram

You can use the central topology diagram of the switch to locate and edit the settings for distributed port groups and uplink groups associated with multiple hosts. You can initiate migration of virtual machine adapters from a port group to a destination on the same or different switch. You can also reorganize the hosts and their networking on the switch by using the **Add and Manage Hosts** wizard.

Topology Diagram of a Host Proxy Switch

The topology diagram of a host proxy switch shows the adapters attached to the switch ports on the host. You can edit the settings of the VMkernel and physical adapters.

Diagram Filters

You can use diagram filters to limit the information displayed in topology diagrams. The default filter limits the topology diagram to display 32 port groups, 32 hosts, and 1024 virtual machines.

You can change the scope of the diagram by using no filters or by applying custom filters. By using a custom filter, you can view information only about a set of virtual machines, a set of port groups on certain hosts, or a port. You can create filters from the central topology diagram of the distributed switch.

View the Topology of a vSphere Distributed Switch

Examine the organization of components that are connected to the distributed switch across the hosts in a vCenter Server.

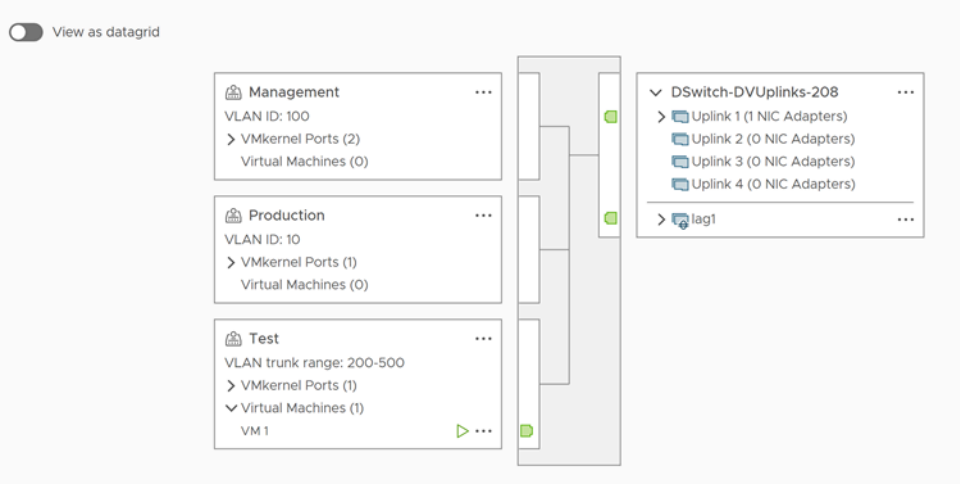
1. Navigate to the vSphere distributed switch in the vSphere Client.
2. On the **Configure** tab, expand **Settings** and select **Topology**.

By default the diagram shows up to 32 distributed port groups, 32 hosts, and 1024 virtual machines.

Diagram of a Distributed Switch That Connects the VMkernel and Virtual Machines to the Network

In your virtual environment, a vSphere Distributed Switch handles VMkernel adapters for vSphere vMotion and for the management network, and virtual machines grouped. You can use the central topology diagram to examine whether a virtual machine or VMkernel adapter is connected to the external network and to identify the physical adapter that carries the data.

Figure 54: Topology Diagram of a Distributed Switch That Handles VMkernel and Virtual Machine Networking



You can perform the following common tasks in the topology of the distributed switch:

- Use filters to view the networking components only for selected port groups on certain hosts, for selected virtual machines, or for a port.
- Locate, configure and migrate virtual machine networking components across host and port groups by using the **Migrate Virtual Machine Networking** wizard.
- Detect the virtual machine adapters that have no network assigned and move them to the selected port group by using the **Migrate Virtual Machine Networking** wizard.
- Handle networking components on multiple hosts by using the **Add and Manage Hosts** wizard.
- View the physical NIC or NIC team that carries the traffic related to a selected virtual machine adapter or VMkernel adapter.

  In this way you can also view the host on which a selected VMkernel adapter resides. Select the adapter, trace the route to the associated physical NIC, and view the IP address or domain name next to the NIC.
- Determine the VLAN mode and ID for a port group. For information about VLAN modes, see VLAN Configuration.

View the Topology of a Host Proxy Switch

Examine and reorganize the networking of the VMkernel and virtual machines that the vSphere Distributed Switch handles on a host.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the distributed switch from the list.

The topology of the host proxy switch appears under the list.

Setting Up VMkernel Networking

You set up VMkernel adapters to provide network connectivity to hosts and to accommodate system traffic of vMotion, IP storage, Fault Tolerance logging, vSAN, and so on.

VMkernel Networking Layer

The VMkernel networking layer provides connectivity to hosts and handles the standard system traffic of vSphere vMotion, IP storage, Fault Tolerance, vSAN, and others. You can also create VMkernel adapters on the source and target vSphere Replication hosts to isolate the replication data traffic.

Multihoming in the VMkernel networking is defined as multiple VMkernel adapters in a TCP/IP stack.

Note: If there is a single vmnic with multiple TCP/IP stacks, it cannot be defined as multihoming.

Multihoming is supported if the vmknics are in different IP subnets. The admin must ensure that the route entries reflect the intent. The ESXi does not run any routing protocol and it does not support or add dynamic routes. For any specific route entry, it must be added statically from the vCenter or the ESXi host. Configurations with more than one vmknic interface on the same IP subnet in a single network stack instance is not supported. Deploying such a configuration might lead to unexpected results like connectivity issues, low throughput and asymmetric routing. However, there are a few exceptions to this rule. For example, iSCSI, Multi-NIC vMotion, and NSX VTEPS. For more information, see http://kb.vmware.com/kb/2010877.

TCP/IP Stacks at the VMkernel Level

Default TCP/IP stack	Provides networking support for the management traffic between vCenter Server and ESXi hosts, and for system traffic such as vMotion, IP storage, Fault Tolerance, and so on.
vMotion TCP/IP stack	Supports the traffic for live migration of virtual machines. Use the vMotion TCP/IP to provide better isolation for the vMotion traffic. After you create a VMkernel adapter on the vMotion TCP/IP stack, you can use only this stack for vMotion on this host. The VMkernel adapters on the default TCP/IP stack are disabled for the vMotion service. If a live migration uses the default TCP/IP stack while you configure VMkernel adapters with the vMotion TCP/IP stack, the migration completes successfully. However, the involved VMkernel adapters on the default TCP/IP stack are disabled for future vMotion sessions.
Provisioning TCP/IP stack	Supports the traffic for virtual machine cold migration, cloning, and snapshot migration. You can use the provisioning TCP/IP to handle Network File Copy (NFC) traffic during long-distance vMotion. NFC provides a file-specific FTP service for vSphere. ESXi uses NFC for copying and moving data between datastores. VMkernel adapters configured with the provisioning TCP/IP

	stack handle the traffic from cloning the virtual disks of the migrated virtual machines in long-distance vMotion. By using the provisioning TCP/IP stack, you can isolate the traffic from the cloning operations on a separate gateway. After you configure a VMkernel adapter with the provisioning TCP/IP stack, all adapters on the default TCP/IP stack are disabled for the Provisioning traffic.
Custom TCP/IP stacks	You can add custom TCP/IP stacks at the VMkernel level to handle networking traffic of custom applications.

Securing System Traffic

Take appropriate security measures to prevent unauthorized access to the management and system traffic in your vSphere environment. For example, isolate the vMotion traffic in a separate network that includes only the ESXi hosts that participate in the migration. Isolate the management traffic in a network that only network and security administrators can access. For more information, see *vSphere Security* and *vSphere Installation and Setup*.

System Traffic Types

Dedicate a separate VMkernel adapter for every traffic type . For distributed switches, dedicate a separate distributed port group for each VMkernel adapter.

Management traffic	Carries the configuration and management communication for ESXi hosts, vCenter Server, and host-to-host High Availability traffic. By default, when you install the ESXi software, a vSphere Standard switch is created on the host together with a VMkernel adapter for management traffic. To provide redundancy, you can connect two or more physical NICs to a VMkernel adapter for management traffic.
vMotion traffic	Accommodates vMotion. A VMkernel adapter for vMotion is required both on the source and the target hosts. Configure The VMkernel adapters for vMotion to handle only the vMotion traffic. For better performance, you can configure multiple NIC vMotion. To have multi-NIC vMotion, you can dedicate two or more port groups to the vMotion traffic, respectively every port group must have a vMotion VMkernel adapter associated with it. Then you can connect one or more physical NICs to every port group. In this way, multiple physical NICs are used for vMotion, which results in greater bandwidth . **Note:** vMotion network traffic is not encrypted. You should provision secure private networks for use by vMotion only.
Provisioning traffic	Handles the data that is transferred for virtual machine cold migration, cloning, and snapshot migration.
IP storage traffic and discovery	Handles the connection for storage types that use standard TCP/IP networks and depend on the VMkernel networking. Such storage types are software iSCSI, dependent hardware iSCSI, and NFS. If you have two or more physical NICs for iSCSI, you can configure iSCSI multipathing. ESXi hosts support NFS 3 and 4.1. To configure a software Fibre Channel over Ethernet (FCoE) adapter, you must have a dedicated VMkernel adapter. Software FCoE passes configuration information though the Data Center Bridging Exchange (DCBX) protocol by using the Cisco Discovery Protocol (CDP)VMkernel module.

Fault Tolerance traffic	Handles the data that the primary fault tolerant virtual machine sends to the secondary fault tolerant virtual machine over the VMkernel networking layer. A separate VMkernel adapter for Fault Tolerance logging is required on every host that is part of a vSphere HA cluster.
vSphere Replication traffic	Handles the outgoing replication data that the source ESXi host transfers to the vSphere Replication server. Dedicate a VMkernel adapter on the source site to isolate the outgoing replication traffic.
vSphere Replication NFC traffic	Handles the incoming replication data on the target replication site.
vSAN traffic	Every host that participates in a vSAN cluster must have a VMkernel adapter to handle the vSAN traffic.
vSphere Backup NFC	VMKernel port setting for dedicated backup NFC traffic. NFC traffic goes through the VMKernel Adapter when vSphereBackup NFC service is enabled.
NVMe over TCP	VMkernel port setting for dedicated NVMe over TCP storage traffic. NVMe over TCP storage traffic goes through the VMkernel Adapter when NVMe over TCP adapter is enabled. For more information see *vSphere Storage Guide*.
NVMEe over RDMA	VMkernel port setting for dedicated NVMe over RDMA storage traffic. NVMe over RDMA storage traffic goes through the VMkernel Adapter when NVMe over RDMA adapter is enabled. For more information, see *vSphere Storage Guide*.

Related Links

Create a vSphere Standard Switch on page 2149

Create a vSphere Standard Switch to provide network connectivity for hosts, virtual machines, and to handle VMkernel traffic. Depending on the connection type that you want to create, you can create a new vSphere Standard Switch with a VMkernel adapter, only connect physical network adapters to the new switch, or create the switch with a virtual machine port group.

View Information About VMkernel Adapters on a Host

You can view each VMkernel adapter's assigned services, associated switch, port settings, IP settings, TCP/IP stack, VLAN ID, and policies.

1. In the vSphere Client, navigate to the host.
2. Click the **Configure** tab and expand the **Networking** menu.
3. To view information about all VMkernel adapters on the host, select **VMkernel adapters**.
4. Select an adapter from the VMkernel adapters list to view its settings.

Tab	Description
All	Displays all configuration information about the VMkernel adapter. This information includes port and NIC settings, IPv4 and IPv6 settings, traffic shaping, teaming and failover, and security policies.
Properties	Displays the port properties and NIC settings of the VMkernel adapter. The port properties include the port group (network label) to which the adapter is associated, the VLAN ID, and the enabled services. The NIC settings include MAC address and the configured MTU size.

Tab	Description
IP Settings	Displays all IPv4 and IPv6 settings for the VMkernel adapter. IPv6 information is not displayed if IPv6 has not been enabled on the host.
Policies	Displays the configured traffic shaping, teaming and failover, and security policies that apply for the port group to which the VMkernel adapter is connected.

Create a VMkernel Adapter on a vSphere Standard Switch

Create a VMkernel network adapter on a vSphere standard switch to provide network connectivity for hosts and to handle the system traffic for vSphere vMotion, IP storage, Fault Tolerance logging, vSAN, and so on. You can also create VMkernel adapters on the source and target vSphere Replication hosts to isolate the replication data traffic. Dedicate a VMkernel adapter to only one traffic type.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **VMkernel adapters**.
3. Click **Add networking**.
4. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
5. On the Select target device page, select either an existing standard switch or select **New standard switch**.
6. Optional: On the Create a Standard Switch page, assign physical NICs to the switch.

   You can create the standard switch without physical NICs and configure them later. During the time that no physical NICs are attached to the host, the host does not have network connectivity to the other hosts on the physical network. The virtual machines on the host are able to communicate with each other.

   a) Click **Add adapters** and select as many physical NICs as you need.
   b) Use the up and down arrows to configure the active and standby NICs.
7. On the Port properties page, configure the settings for the VMkernel adapter.

Option	Description
Network label	The network label is inherited from the label of the distributed port group.
IP settings	Select IPv4, IPv6, or both. **Note:** The IPv6

Option	Description
	option does not appear on hosts that do not have IPv6 enabled.
MTU	Choose whether to get MTU for the network adapter from the switch or to set a custom size. You cannot set the MTU size to a value greater than 9000 bytes.
TCP/IP stack	Select a TCP/IP stack from the list. Once

Option	Description
	you set a TCP/IP stack for the VMkernel adapter, you cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you will be able to use only these stacks to handle vMotion or Provisioning traffic on the host. All VMkernel adapters for vMotion on the default

Option	Description
	TCP/IP stack are deactivated for future vMotion sessions. If you set the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are deactivated for operations that include Provisioning traffic, such as virtual machine cold migration, cloning, and snapshot migration.
Available services	You can enable services for the default TCP/IP

Option	Description
	stack on the host. Select from the available services: • **vMotion**. Enables the VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. The migration with vMotion to the selected host is not possible if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack,

Option	Description
	or there are no adapters using the vMotion TCP/IP stack. • **Provisio** Handles the data transferre for virtual machine cold migration cloning, and snapshot migration • **Fault Toleranc logging**. Enables Fault Tolerance logging on the host. You can use only one VMkerne adapter for FT traffic per host. • **Manager** Enables the managem traffic for the host and vCenter

Option	Description
	Server. Typically, hosts have such a VMkerne adapter created when the ESXi software is installed. You can create another VMkerne adapter for managen traffic on the host to provide redundar • **vSphere Replicati** Handles the outgoing replicatio data that is sent from the source ESXi host to the vSphere Replicati server. • **vSphere Replicati NFC**. Handles the incoming replicatio

Option	Description
	data on the target replicatio site. • **vSAN**. Enables the vSAN traffic on the host. Every host that is part of a vSAN cluster must have such a VMkerne adapter. • **vSphere Backup NFC**. VMkerne port setting for dedicate backup NFC traffic. NFC traffic goes through the VMkerne Adapter when vSphereE NFC service is enabled. • **NVMe over TCP**. VMkerne

Option	Description
	port setting for dedicated NVMe over TCP storage traffic. NVMe over TCP storage traffic goes through the VMkerne Adapter when NVMe over TCP adapter is enabled. For more informati see *vSphere Storage Guide*. • **NVMe over RDMA**. VMkerne port setting for dedicated NVMe over RDMA storage traffic. NVMe over RDMA storage traffic goes through the VMkerne Adapter when

Option	Description
	NVMe over RDMA adapter is enabled. For more informatio see *vSphere Storage Guide*.

8. Optional: On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are

Option	Description
	obtained from the selected TCP/IP stack. Select the **Override default gateway for this adapter** check box and enter a gateway address, if you want to specify a different gateway for the VMkernel adapter. **Note:** Selected netstack should have the default gateway explicitly on each host.

9. Optional: On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses.

Option	Description
	A DHCPv6 server must be present on the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisemer to obtain IPv6 addresses. In ESXi 6.5 and later router advertisemer is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	1. Click **Add IPv6 address** to add a new IPv6 address. 2. Enter the IPv6 address and

Option	Description
	subnet prefix length, and click **OK**. 3. To change the VMkernel default gateway, click **Override default gateway for this adapter**. The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

10. Review your settings selections on the Ready to complete page and click **Finish**.

Related Links

Create a vSphere Standard Switch on page 2149

Create a vSphere Standard Switch to provide network connectivity for hosts, virtual machines, and to handle VMkernel traffic. Depending on the connection type that you want to create, you can create a new vSphere Standard Switch with a VMkernel adapter, only connect physical network adapters to the new switch, or create the switch with a virtual machine port group.

Create a VMkernel Adapter on a Host Associated with a vSphere Distributed Switch

Create a VMkernel adapter on a host that is associated with a distributed switch to provide network connectivity to the host and to handle the traffic for vSphere vMotion, IP storage, Fault Tolerance logging, vSAN, and others. You can set up VMkernel adapters for the standard system traffic on vSphere standard switches and on vSphere distributed switches.

You should dedicate a single distributed port group per VMkernel adapter. For better isolation, you should configure one VMkernel adapter with one traffic type.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **VMkernel adapters**.
3. Click **Add networking**.
4. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
5. From the **Select an existing network** option, select a distributed port group and click **Next**.
6. On the Port properties page, configure the settings for the VMkernel adapter.

Option	Description
Network label	The network label is inherited from the label of the distributed port group.
IP settings	Select IPv4, IPv6, or both. **Note:** The IPv6 option does not appear on hosts that do not have IPv6 enabled.

Option	Description
MTU	Choose whether to get MTU for the network adapter from the switch or to set a custom size. You cannot set the MTU size to a value greater than 9000 bytes.
TCP/IP stack	Select a TCP/IP stack from the list. Once you set a TCP/IP stack for the VMkernel adapter, you

Option	Description
	cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you will be able to use only these stacks to handle vMotion or Provisioning traffic on the host. All VMkernel adapters for vMotion on the default TCP/IP stack are deactivated for future vMotion sessions. If you

Option	Description
	set the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are deactivated for operations that include Provisioning traffic, such as virtual machine cold migration, cloning, and snapshot migration.
Available services	You can enable services for the default TCP/IP stack on the host. Select from the available services: • **vMotion**. Enables the

Option	Description
	VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. The migration with vMotion to the selected host is not possible if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or there are no adapters using the vMotion TCP/IP stack.

Option	Description
	• **Provisio** Handles the data transferre for virtual machine cold migration cloning, and snapshot migration • **Fault Toleranc logging**. Enables Fault Tolerance logging on the host. You can use only one VMkerne adapter for FT traffic per host. • **Manager** Enables the managem traffic for the host and vCenter Server. Typically, hosts have such a VMkerne adapter created when the

Option	Description
	ESXi software is installed. You can create another VMkerne adapter for managen traffic on the host to provide redundar • **vSphere Replicati** Handles the outgoing replicatio data that is sent from the source ESXi host to the vSphere Replicati server. • **vSphere Replicati NFC**. Handles the incoming replicatio data on the target replicatio site. • **vSAN**. Enables the vSAN traffic

Option	Description
	on the host. Every host that is part of a vSAN cluster must have such a VMkerne adapter. • **vSphere Backup NFC**. VMkerne port setting for dedicated backup NFC traffic. NFC traffic goes through the VMkerne Adapter when vSphereB NFC service is enabled. • **NVMe over TCP**. VMkerne port setting for dedicated NVMe over TCP storage traffic. NVMe over

Option	Description
	TCP storage traffic goes through the VMkerne Adapter when NVMe over TCP adapter is enabled. For more informati see *vSphere Storage Guide*. • **NVMe over RDMA**. VMkerne port setting for dedicate NVMe over RDMA storage traffic. NVMe over RDMA storage traffic goes through the VMkerne Adapter when NVMe over RDMA adapter is enabled. For more informati see *vSphere*

Option	Description
	Storage Guide.

7. Optional: On the IPv4 settings page, select an option for obtaining IP addresses.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack. Select the **Override default**

Option	Description
	gateway for this adapter check box and enter a gateway address, if you want to specify a different gateway for the VMkernel adapter. **Note:** Selected netstack should have the default gateway explicitly on each host.

8. Optional: On the IPv6 settings page, select an option for obtaining IPv6 addresses.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.

Option	Description
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisemer to obtain IPv6 addresses. In ESXi 6.5 and later router advertisemer is enabled by default and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	1. Click **Add IPv6 address** to add a new IPv6 address. 2. Enter the IPv6 address and subnet prefix length, and click **OK**. 3. To change the VMkerne

Option	Description
	default gateway, click **Override default gateway for this adapter**. The VMkernel Default Gateway address for IPv6 is obtained from the selected TCP/IP stack.

9. Review your settings selections on the Ready to complete page and click **Finish**.

Edit a VMkernel Adapter Configuration

You might have to change the supported traffic type for a VMkernel adapter, or the way IPv4 or IPv6 addresses are obtained.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **VMkernel adapters**.
3. Select the VMkernel adapter that resides on the target distributed or standard switch and click **Edit**.
4. On the Port properties page, edit the settings for the VMkernel adapter.

Option	Description
MTU	Choose whether to get MTU for the network adapter from the switch or to set a custom size. You cannot set the MTU size to a value greater than 9000 bytes.
TCP/IP stack	Select a TCP/IP stack from the list. Once you set a TCP/IP stack for the VMkernel adapter, you cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you will be able to use only these stacks to handle vMotion or Provisioning traffic on the host. All VMkernel adapters for vMotion on the default TCP/IP stack are disabled for future vMotion sessions. If you set the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are disabled for operations that include Provisioning traffic, such as virtual machine cold migration, cloning, and snapshot migration.
Available services	You can enable services for the default TCP/IP stack on the host. Select from the available services:

Option	Description
	• **vMotion**. Enables the VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. The migration with vMotion to the selected host is not possible if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or there are no adapters using the vMotion TCP/IP stack. • **Provisioning**. Handles the data transferred for virtual machine cold migration, cloning, and snapshot migration. • **Fault Tolerance logging**. Enables Fault Tolerance logging on the host. You can use only one VMkernel adapter for FT traffic per host. • **Management**. Enables the management traffic for the host and vCenter Server. Typically, hosts have such a VMkernel adapter created when the ESXi software is installed. You can create another VMkernel adapter for management traffic on the host to provide redundancy. • **vSphere Replication**. Handles the outgoing replication data that is sent from the source ESXi host to the vSphere Replication server. • **vSphere Replication NFC**. Handles the incoming replication data on the target replication site. • **vSAN**. Enables the vSAN traffic on the host. Every host that is part of a vSAN cluster must have such a VMkernel adapter. • **vSphere Backup NFC**. VMKernel port setting for dedicated backup NFC traffic. NFC traffic goes through the VMKernel Adapter when vSphereBackup NFC service is enabled. • **NVMe over TCP**. VMKernel port setting for dedicated NVMe over TCP storage traffic. NVMe over TCP storage traffic goes through the VMKernel Adapter when NVMe over TCP adapter is enabled. For more information, see *vSphere Storage Guide*. • **NVMe over RDMA**. VMKernel port setting for dedicated NVMe over RDMA storage traffic. NVMe over RDMA storage traffic goes through the VMKernel Adapter when NVMe over RDMA adapter is enabled. For more information, see *vSphere Storage Guide*.

5. Optional: On the IPv4 settings page, select the method by which IP addresses are obtained.

Option	Description
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings. A DHCP server must be present on

Option	Description
	the network.
Use static IPv4 settings	Enter the IPv4 IP address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack. Select the **Override default gateway for this adapter** check box and enter a gateway address, if you want to specify a different gateway for

Option	Description
	the VMkernel adapter. **Note:** Selected netstack should have the default gateway explicitly on each host.

6. Optional: On the IPv6 settings page, select an option for obtaining IPv6 addresses.

   Note: The IPv6 option does not appear on hosts that do not have IPv6 enabled.

Option	Description
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisemer to obtain IPv6 addresses. In ESXi 6.5 and later router advertisemer is enabled by default

Option	Description
	and supports the M and O flags in accordance with RFC 4861.
Static IPv6 addresses	1. Click **Add IPv6 address** to add a new IPv6 address. 2. Enter the IPv6 address and subnet prefix length, and click **OK**. 3. To change the VMkerne default gateway, click **Override default gateway for this adapter**. The VMkernel Default Gateway address for IPv6 is obtained from

Option	Description
	the selected TCP/IP stack.

7. Click **OK**.

Overriding the Default Gateway of a VMkernel Adapter

You might need to override the default gateway for a VMkernel adapter to provide a different gateway for vSphere vMotion.

Each TCP/IP stack on a host can have only one default gateway. This default gateway is part of the routing table and all services that operate on the TCP/IP stack use it.

For example, the VMkernel adapters vmk0 and vmk1 can be configured on a host.

- vmk0 is used for management traffic on the 10.162.10.0/24 subnet, with default gateway 10.162.10.1
- vmk1 is used for vMotion traffic on the 172.16.1.0/24 subnet

If you set 172.16.1.1 as the default gateway for vmk1, vMotion uses vmk1 as its egress interface with the gateway 172.16.1.1. The 172.16.1.1 gateway is a part of the vmk1 configuration and is not in the routing table. Only the services that specify vmk1 as an egress interface use this gateway. This provides additional Layer 3 connectivity options for services that need multiple gateways.

You can use the vSphere Client or an ESXCLI command to configure the default gateway of a VMkernel adapter.

See Create a VMkernel Adapter on a vSphere Standard Switch, Create a VMkernel Adapter on a Host Associated with a vSphere Distributed Switch, and Configure the VMkernel Adapter Gateway by Using esxcli Commands.

Configure the VMkernel Adapter Gateway by Using esxcli Commands

You can override the default gateway of a VMkernel adapter to provide a different gateway for vSphere vMotion by using esxcli commands.

1. Open an SSH connection to the host.
2. Log in as the root user.
3. Run the following command.

Option	Description
IPv4	`esxcli network ip interface ipv4 set -i vmknic -t static -g IPv4 gateway -I IPv4 address -N mask`

IPv6	**Important:** You must turn off DHCPv6 or Router Advertisement before you can set the IPv6 vmknic gateway.
	`esxcli network ip interface ipv6 set -i vmknic -d off -r off`
	To add a static IPv6 address:
	`esxcli network ip interface ipv6 address add -i vmknic -I IPv6 address`
	To set the IPv6 vmknic gateway:

Option	Description
	`esxcli network ip interface ipv6 set -i vmknic -g IPv6 gateway`

Where *vmknic* is the name of the VMkernel adapter, *gateway* is the IP address of the gateway, *IP address* is the address of the VMkernel adapter, and *mask* is the network mask.

Configure the resolv.conf File by Using esxcli Commands

The `resolv.conf` file is used to configure centrally managed DNS servers. You can configure entries in the `/etc/resolv.conf` file using `esxcli` commands, which allows the modification to remain when rebooting the ESXi host. The property can be set explicitly if DHCP is not enabled.

1. Open an SSH connection to the host.
2. Log in as the root user.
3. Run the following command.

Option	Description

Add DNS server	To add a new DNS server to the end of the list of DNS servers to use for this ESXi host.
	`esxcli network ip dns server add`
	Command Options
	`-N|--netstack=<str>`
	The network stack instance. If it is not specified, then use the default netstack instance.
	`-s|--server=<str>`
	The IPV4 or the IPV6 address of the DNS server that you want to add to the DNS server list.
	Note: This command is required.
	`For example: esxcli network ip dns server add -N vmotion -s xx.xx.xx.xx`

Add DNS search	To add a search domain to the list of domains to be searched when trying to resolve a host name on the ESXi host.
	`esxcli network ip dns search add`
	Command Options
	`-d|--domain=<str>`
	The string name of a domain that you want to add to the list of search domains.
	Note: This command is required.
	`-N|--netstack=<str>`
	The network stack instance. If it is not specified, then use the default netstack instance.

Remove DNS server	To remove a DNS server from the list of DNS servers to use for this ESXi host.
	`esxcli network ip dns server remove`*IP address*
	Command Options
	`-a|--all`
	`-N|--netstack=<str>`
	The network stack instance. If it is not specified, then use the default netstack instance.
	`-s|--server=<str>`

Option	Description

Remove DNS search	To remove a search domain to the list of domains to be searched when trying to resolve an host name on the ESXi host.
	`esxcli network ip dns search remove`
	Command Options
	`-d|--domain=<str>`
	The string name of a domain that you want to remove from the list of search domains.
	Note: This command is required.
	`-N|--netstack=<str>`
	The network stack instance. If it is not specified, then use the default netstack instance.

List DNS search	To print a list the DNS server currently configured on the system in the order in which they will be used.
	`esxcli network ip dns server list`
	Command Options
	`-N|--netstack=<str>`
	The network stack instance. If it is not specified, then use the default netstack instance.
	`For example: esxcli network ip dns server list -N vmotion`

List DNS search domain	To list the search domains currently configured on the ESXi host in the order in which they will be used while searching.
	`esxcli network ip dns search list -N`
	Command Options
	`---N|--netstack=<str>`
	The network stack instance. If it is not specified, then use the default netstack instance.
	`For example: esxcli network ip dns search list -N vmotion`

Configure the DNS Hosts File by Using ESXCLI Commands

The DNS hosts file is used for mapping hostnames or domain names to IP addresses. You can configure entries in the `/etc/hosts` file using `esxcli` commands, which allows the modifications to remain unchanged while rebooting the ESXi host.

1. Open an SSH connection to the host.
2. Log in as the root user.
3. Run the following command.

Option	Description

add	To add the hostname and IP address mapping, run the following command.
	`esxcli network ip hosts add --ip --hostname`
	`For example: esxcli network ip hosts add --hostname www.samplehostname.com --ip xx.xx.xx.xx`

remove	To remove a hostname mapping from the configuration, run the following command. `esxcli network ip hosts remove --hostname`

Option	Description
	`For example: esxcli network ip hosts remove --host-name www.samplehostname.com --ip xx.xx.xx.xx`
list	To list the IP addresses and their associated DNS entries, run the following command. `esxcli network ip hosts list`

Where *`IP address`* is the address of the VMkernel adapter, *`hostname`* is the DNS entry you want to associate with the IP address, *`alaises`* is any aliases you want to associate, and *`comment`* is a line about this entry.

Note: ESXCLI network IP hosts add values only to the other hosts. The ESXCLI network IP host does not add values to the current host. The information about the current host is managed through the host name under the **Network Settings**. If you try to change the current hostname you might see an error similar to the following:

```
Error adding etc host item: User can not set item for management IP: X.X.X.X
```

For information on changing the host name of the current host, see Change the Configuration of a TCP/IP Stack on a Host.

View TCP/IP Stack Configuration on a Host

You can view the DNS and routing configuration of a TCP/IP stack on a host. You can also view the IPv4 and IPv6 routing tables, the congestion control algorithm, and the maximum number of allowed connections.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **TCP/IP configuration**.
3. Select a stack from the TCP/IP Stacks table.

   If no custom TCP/IP stacks are configured on the host, you view the default, vMotion, and Provisioning TCP/IP stacks on the host.

DNS and routing details about the selected TCP/IP stack appear below the TCP/IP Stacks table. You can view the IPv4 and IPv6 routing tables, and the DNS and routing configuration for the stack.

Note: The IPv6 routing table is only visible if IPv6 is enabled on the host.

The **Advanced** tab contains information about the configured congestion control algorithm and the maximum number of allowed connections to the stack.

Change the Configuration of a TCP/IP Stack on a Host

You can change the DNS and default gateway configuration of a TCP/IP stack on a host. You can also change the congestion control algorithm, the maximum number of connections, and the name of custom TCP/IP stacks.

Note: You can change the DNS and default gateway configuration of the default TCP/IP stack only. Multiple DNS and gateways configurations are supported when using separate TCP/IP stacks.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **TCP/IP configuration**.
3. Select a stack from the table, click **Edit** and make the appropriate changes.

Page	Option
DNS Configuration	Select a method of obtaining the DNS server.

Page	Option
	• Select **Obtain settings automatically from a VMkernel network adapter** and select a network adapter from the **VMKernel network adapter** drop-down menu • Select **Enter settings manually** and edit the DNS configuration settings. a. Edit the Host name. b. Edit the Domain name. c. Type a preferred DNS server IP address. d. Type an alternate DNS server IP address. e. Use the **Search domains** text box to specify DNS suffixes to use in DNS search when resolving unqualified domain names.
Routing	Edit the VMkernel gateway information. **Note:** Removing the default gateway might cause the client to lose connectivity with the host.
Name	Change the name of a custom TCP/IP stack
Advanced	Edit the maximum number of connections and the congestion control algorithm of the stack

4. Click **OK** to apply your changes.

You can add static routes to additional gateways by using CLI commands. For more information, see http://kb.vmware.com/kb/2001426

Explicit Congestion Notification

Explicit Congestion Notification (ECN) allows a TCP sender to reduce the transmission rate to avoid packet drops. ECN is specified in RFC 3168. vSphere 7.0 and later supports ECN and it is enabled by default.

You can get the ECN status of any netstack using esxcli command.

1. In the ESXi Shell on the host, use the following command.

   ```
   esxcli network ip netstack set -N <NetStack-Name> --ecn=<str>
   ```

2. You can set the status of ECN. The setting has the following possible values in ESXi.

   ```
   ...
     --ecn=<str>           The status of ECN (Explicit Congestion Notification).
                               disabled: Completely disable ECN functionality
                               echo-only: Only echoing ECN, won't initiate
                               enabled: Fully enable ECN functionality
   ```

   The default value of this parameter is enabled. ESXi is likely to use ECN if the value of this parameter is enabled. If a router or a network appliance in the environment cannot handle IP packets with ECN bits accurately, then the ECN capability can be set to disabled.

Create a Custom TCP/IP Stack

You can create a custom TCP/IP stack on a host to forward networking traffic through a custom application.

Once you set a TCP/IP stack for the VMkernel adapter, you cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you can use only these stacks to handle vMotion or Provisioning traffic on the host. All VMkernel adapters for vMotion on the default TCP/IP stack are disabled for future vMotion sessions. If you set the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are disabled for operations that include Provisioning traffic, such as virtual machine cold migration, cloning, and snapshot migration.

If you must change the TCP/IP stack configuration, delete the existing VMkernel adapter and create a new one. You can then create a TCP/IP stack for that adapter.

1. Open an SSH connection to the host.
2. Log in as the root user.
3. Run the ESXCLI command.

```
esxcli network ip netstack add -N="stack_name"
```

The custom TCP/IP stack is created on the host. You can assign VMkernel adapters to the stack.

Remove a VMkernel Adapter

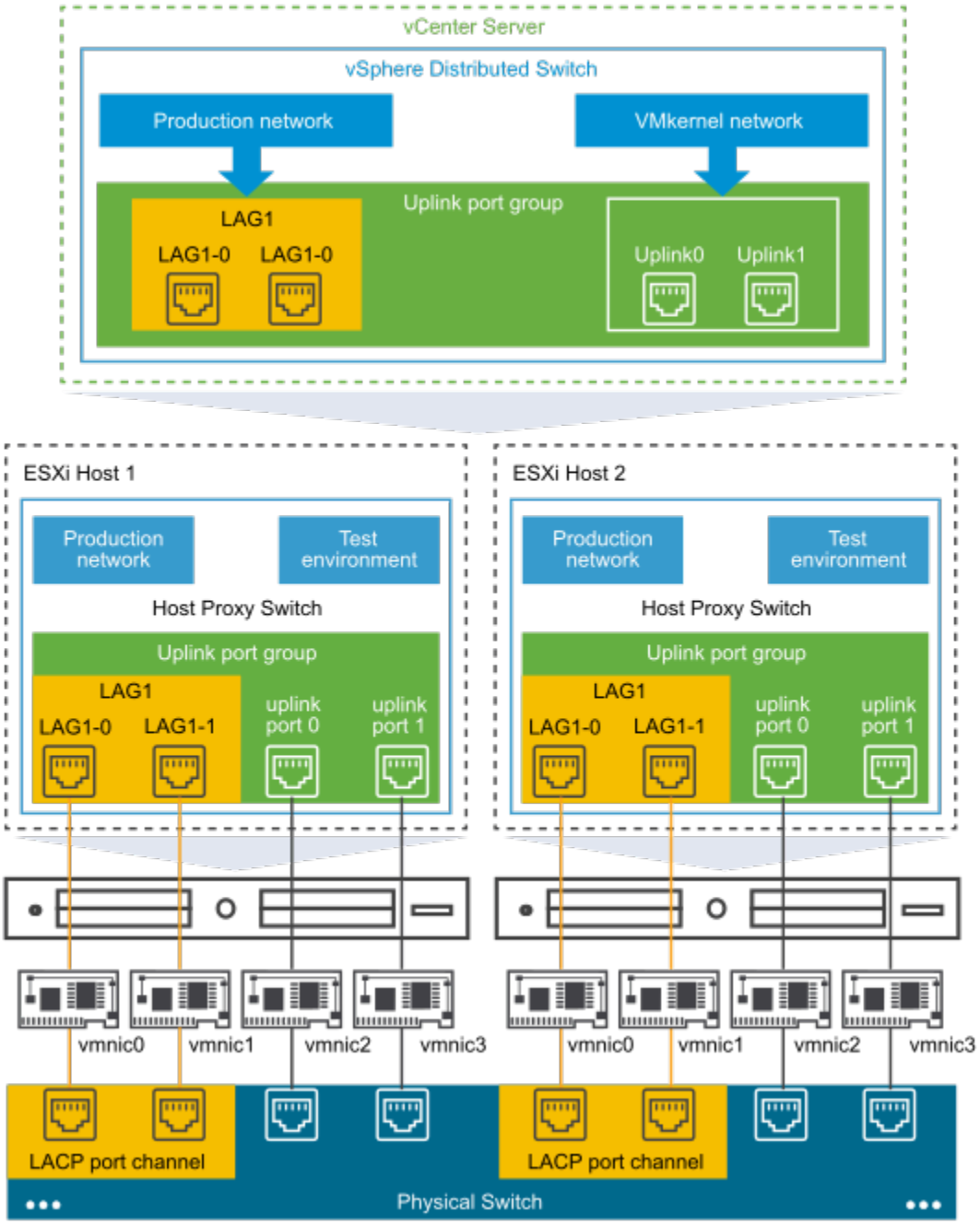
Remove a VMkernel adapter from a vSphere distributed or a standard switch when you no longer need the adapter. Make sure that you leave at least one VMkernel adapter for management traffic on the host to keep the network connectivity up.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **VMkernel adapters**.
3. Select a VMkernel adapter from the list, and click the **Remove selected network adapter** icon.
4. Click **Remove**.

LACP Support on a vSphere Distributed Switch

With link aggregation control protocol (LACP) support on a vSphere Distributed Switch, you can connect ESXi hosts to physical switches by using dynamic link aggregation. You can create multiple link aggregation groups (LAGs) on a distributed switch to aggregate the bandwidth of physical NICs on ESXi hosts that are connected to LACP port channels.

Figure 55: Enhanced LACP Support on a vSphere Distributed Switch



LACP Configuration on the Distributed Switch

You configure a LAG with two or more ports and connect physical NICs to the ports. LAG ports are teamed within the LAG, and the network traffic is load balanced between the ports through an LACP hashing algorithm. You can use a LAG to handle the traffic of distributed port groups to provide increased network bandwidth, redundancy, and load balancing to the port groups.

When you create a LAG on a distributed switch, a LAG object is also created on the proxy switch of every host that is connected to the distributed switch. For example, if you create LAG1 with two ports, LAG1 with the same number of ports is created on every host that is connected to the distributed switch.

On a host proxy switch, you can connect one physical NIC to only one LAG port. On the distributed switch, one LAG port can have multiple physical NICs from different hosts connected to it. The physical NICs on a host that you connect to the LAG ports must be connected to links that participate in an LACP port channel on the physical switch.

You can create up to 64 LAGs on a distributed switch. A host can support up to 32 LAGs. However, the number of LAGs that you can actually use depends on the capabilities of the underlying physical environment and the topology of the virtual network. For example, if the physical switch supports up to four ports in an LACP port channel, you can connect up to four physical NICs per host to a LAG.

You can configure LACP timeout value. LACP functions by sending frames down all the links that have the protocol enabled. If it finds a device on the other end of the link that also has LACP enabled, it sends frames independently along the same links, enabling the two units to detect multiple links between themselves and then combine them into a single logical link. The timeout value is the amount of time that a LAG interface waits for a Protocol Data Unit (PDU) from the remote system before bringing the LACP session down. Periodic transmissions of LACP PDUs occur at either a slow or fast transmission rate.

Port Channel Configuration on the Physical Switch

For each host on which you want to use LACP, you must create a separate LACP port channel on the physical switch. You must consider the following requirements when configuring LACP on the physical switch:

- The number of ports in the LACP port channel must be equal to the number of physical NICs that you want to group on the host. For example, if you want to aggregate the bandwidth of two physical NICs on a host, you must create an LACP port channel with two ports on the physical switch. The LAG on the distributed switch must be configured with at least two ports.
- The hashing algorithm of the LACP port channel on the physical switch must be the same as the hashing algorithm that is configured to the LAG on the distributed switch.
- All physical NICs that you want to connect to the LACP port channel must be configured with the same speed and duplex.

Configure LACP Teaming and Failover for Distributed Port Groups

To handle the network traffic of distributed port groups by using a LAG, you assign physical NICs to the LAG ports and set the LAG as active in the teaming and failover order of distributed port groups.

Table 180: LACP Teaming and failover configuration of distributed port groups

Failover Order	Uplinks	Description
Active	A single LAG	You can only use one active LAG or multiple standalone uplinks to handle the traffic of distributed port groups . You cannot configure multiple active LAGs or mix active LAGs and standalone uplinks.
Standby	Empty	Having an active LAG and standby uplinks and the reverse is not supported. Having a LAG and another standby LAG is not supported.
Unused	All standalone uplinks and other LAGs if any	Because only one LAG must be active and the Standby list must be empty, you must set all standalone uplinks and other LAGs to unused.

Configure a Link Aggregation Group to Handle the Traffic for Distributed Port Groups

To aggregate the bandwidth of multiple physical NICs on hosts, you can create a link aggregation group (LAG) on the distributed switch and use it to handle the traffic of distributed port groups.

- Verify that for every host where you want to use LACP, a separate LACP port channel exists on the physical switch. See LACP Support on a vSphere Distributed Switch.
- Verify that the vSphere Distributed Switch where you configure the LAG is version 6.5 or later.
- Verify that enhanced LACP is supported on the distributed switch.

Newly created LAGs do not have physical NICs assigned to their ports and are unused in the teaming and failover order of distributed port groups. To handle the network traffic of distributed port groups by using a LAG, you must migrate the traffic from standalone uplinks to the LAG.

Create a Link Aggregation Group

To migrate the network traffic of distributed port groups to a link aggregation group (LAG), you create a LAG on the distributed switch.

1. In the vSphere Client, navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **LACP**.
3. Click the **New Link Aggregation Group** icon.
4. Name the new LAG.
5. Set the number of ports to the LAG.

   Set the same number of ports to the LAG as the number of ports in the LACP port channel on the physical switch. A LAG port has the same function as an uplink on the distributed switch. All LAG ports form a NIC team in the context of the LAG.
6. Select the LACP negotiating mode of the LAG.

Option	Description
Active	All LAG ports are in an Active negotiating mode. The LAG ports initiate negotiations with the LACP port channel on the physical switch by sending LACP packets.
Passive	The LAG ports are in Passive negotiating mode. The LAG ports respond to LACP packets they receive but do not initiate LACP negotiation.

   If the LACP-enabled ports on the physical switch are in Active negotiating mode, you can set the LAG ports in Passive mode and the reverse.
7. Select a load balancing mode from the hashing algorithms that LACP defines.

   Note: The hashing algorithm must be the same as the hashing algorithm set to the LACP port channel on the physical switch.
8. Select the link aggregation timeout mode.

   Periodic transmissions of LACP PDUs occur at either a slow or fast transmission rate, depending upon the LACP timeout preference you select. In a fast timeout, PDUs are sent every second, and, in a slow timeout, PDUs are sent every 30 seconds. A slow timeout is the default setting.

   Note: A fast timeout is supported only on distributed switch version 7.0.2 or later.

9. Set the VLAN and the NetFlow policies for the LAG.

   This option is active when overriding the VLAN and NetFlow policies per individual uplink ports is enabled on the uplink port group. If you set the VLAN and NetFlow policies to the LAG, they override the policies set on the uplink port group level.

10. Click **OK**.

The new LAG is unused in the teaming and failover order of distributed port groups. No physical NICs are assigned to the LAG ports.

As with standalone uplinks, the LAG has a representation on every host that is associated with the distributed switch. For example, if you create LAG1 with two ports on the distributed switch, a LAG1 with two ports is created on every host that is associated with the distributed switch.

Set the LAG as standby in the teaming and failover configuration of distributed port groups. In this way, you create an intermediate configuration that lets you migrate the network traffic to the LAG without losing network connectivity.

Set a LAG as Standby in the Teaming and Failover Order

The new link aggregation group (LAG) by default is unused in the teaming and failover order of distributed port groups. Because only one LAG or only standalone uplinks can be active for distributed port groups, you must create an intermediate teaming and failover configuration, where the LAG is standby. This configuration lets you migrate physical NICs to the LAG ports by keeping the network connectivity up.

1. Navigate to the distributed switch.
2. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**.
3. Select **Teaming and failover** and click **Next**.
4. Select the port groups where you want to use the LAG.
5. In Failover order, select the LAG and use the up arrow to move it to the Standby uplinks list.
6. Click **Next**, review the message that informs you about the usage of the intermediate teaming and failover configuration, and click **OK**.
7. On the Ready to complete page, click **Finish**.

Migrate physical NICs from standalone uplinks to the LAG ports.

Assign Physical NICs to the Ports of the Link Aggregation Group

You have set the new link aggregation group (LAG) as standby in the teaming and failover order of distributed port groups. Having the LAG as standby lets you safely migrate the physical NICs from standalone uplinks to the LAG ports without losing network connectivity.

- Verify that either all LAG ports or the corresponding LACP-enabled ports on the physical switch are in active LACP negotiating mode.

- Verify that the physical NICs that you want to assign to the LAG ports have the same speed and are configured at full duplex.

1. In the vSphere Client, navigate to the distributed switch where the LAG resides.
2. From the **Actions** menu, select **Add and Manage Hosts**.
3. Select **Manage host networking**.
4. Select the host whose physical NICs you want to assign to the LAG ports and click **Next**.
5. On the Select network adapter tasks page, select **Manage physical adapters** and click **Next**.
6. On the Manage physical adapters page, select a NIC and click **Assign an uplink**.
7. Select a LAG port and click **OK**.
8. Repeat 6 and 7 for all physical NICs that you want to assign to the LAG ports.
9. Complete the wizard.

   Configure Two Physical NICs to a LAG in the Add and Manage Hosts Wizard

   For example, if you have a LAG with two ports, you configure a physical NIC to each LAG port in the **Add and Manage Hosts** wizard.

Set the LAG as active and all standalone uplinks to unused in the teaming and failover order of distributed port groups.

Set the Link Aggregation Group as Active in the Teaming and Failover Order of the Distributed Port Group

You migrated physical NICs to the ports of the link aggregation group (LAG). Set the LAG as active and move all standalone uplinks as unused in the teaming and failover order of the distributed port groups.

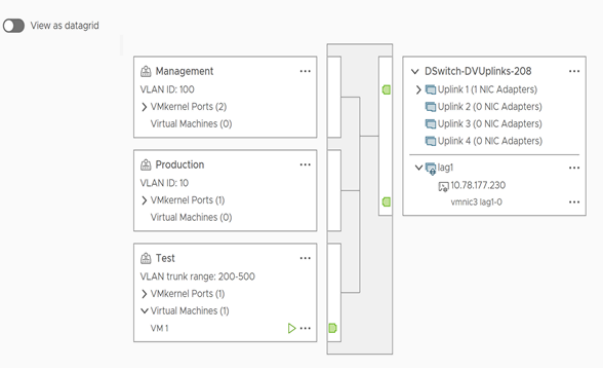
1. Navigate to the distributed switch.
2. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**.
3. Select **Teaming and failover** and click **Next**.
4. Select the port groups where you set the LAG as standby and click **Next**.
5. In Failover order, use the up and down arrows to move the LAG in the Active list, all standalone uplinks in the Unused list, and leave the Standby list empty.
6. Click **Next** and click **Finish**.

You safely migrated network traffic from standalone uplinks to a LAG for distributed port groups and created a valid LACP teaming and failover configuration for the groups.

Topology of a Distributed Switch that Uses a LAG

If you configure a LAG with two ports to handle the traffic of a distributed port group, you can check the topology of the distributed switch to view how it changed as a result of the new configuration.

Figure 56: Distributed Switch Topology with a LAG



Edit a Link Aggregation Group

Edit the settings of a link aggregation group (LAG) if you need to add more ports to the group or change the LACP negotiating mode, the load balancing algorithm, or the VLAN and NetFlow policies.

1. In the vSphere Client, navigate to the vSphere Distributed Switch.
2. On the **Configure** tab, expand **Settings** and select **LACP**.
3. Click the **New Link Aggregation Group** icon.
4. In the **Name** text box, type a new name for the LAG.
5. Change the number of ports for the LAG if you want to add more physical NICs to it.

   The new NICs must be connected to ports that are part of an LACP port channel on the physical switch.
6. Change the LACP negotiating mode of the LAG.

   If all ports on the physical LACP port channel are in Active LACP mode, you can change the LACP mode of the LAG to Passive and the reverse.
7. Change the load balancing mode of the LAG.

   You can select from the load balancing algorithms that LACP defines.
8. Select the link aggregation timeout mode.

   Periodic transmissions of LACP PDUs occur at either a slow or fast transmission rate, depending upon the LACP timeout preference you select. In a fast timeout, PDUs are sent every second, and, in a slow timeout, PDUs are sent every 30 seconds. A slow timeout is the default setting.

   Note: You can set a fast LACP timeout by running the following ESXCLI command. However, the setting is not available against an NSX-T enabled DVS or N-VDS (opaque NSX Distributed vSwitch).

   ```
   esxcli network vswitch dvs vmware lacp timeout set --vds DVS-name --lag-id <integer> --timeout 1
   ```
9. Change the VLAN and the NetFlow policies.

   This option is active when the option for overriding the VLAN and NetFlow policies for individual ports is enabled on the uplink port group. If you change the VLAN and NetFlow policies for the LAG, they override the policies set at the uplink port group level.
10. Click **OK**.

Limitations of the LACP Support on a vSphere Distributed Switch

The LACP support on a vSphere Distributed Switch lets network devices negotiate automatic bundling of links by sending LACP packets to a peer. However, the LACP support on a vSphere Distributed Switch has limitations.

- The LACP is not supported with software iSCSI port binding. iSCSI multipathing over LAG is supported, if port binding is not used.
- The LACP support settings are not available in host profiles.
- The LACP support is not possible between nested ESXi hosts.
- The LACP support does not work with the ESXi dump collector.
- The LACP control packets (LACP PDU) do not get mirrored when port mirroring is enabled.
- The teaming and failover health check does not work for LAG ports. LACP checks the connectivity of the LAG ports.
- The enhanced LACP support works correctly when only one LAG handles the traffic per distributed port or port group.

Backing Up and Restoring Networking Configurations

vSphere enables you to backup and restore the configuration of a vSphere Distributed Switch , distributed and uplink port groups in cases of invalid changes or a transfer to another deployment.

Backing Up and Restoring a vSphere Distributed Switch Configuration

vCenter Server provides the ability to backup and restore the configuration of a vSphere Distributed Switch. You can restore the virtual network configuration in cases of database or upgrade failure. You can also use a saved switch configuration as a template to create a copy of the switch in the same or a new vSphere environment.

You can import or export a configuration of a distributed switch including its port groups. For information about exporting, importing, and restoring a port group configuration, see Export, Import, and Restore vSphere Distributed Port Group Configurations.

Note: You can use a saved configuration file to restore policies and hosts associations on the distributed switch. You cannot restore the connection of physical NICs to uplink ports or ports of link aggregation groups.

Export vSphere Distributed Switch Configurations

You can export vSphere Distributed Switch and distributed port group configurations to a file. The file preserves valid network configurations, enabling transfer of these configurations to other environments.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Settings** > **Export Configuration**.
3. Choose to export the distributed switch configuration, or export the distributed switch configuration and all port groups.
4. Optional: Enter notes about this configuration in the **Descriptions** field.
5. Click **OK.**
6. Click **Yes** to save the configuration file to your local system.

Use the exported configuration file to do the following tasks:

- Create a copy of the exported distributed switch in a vSphere environment. See Import a vSphere Distributed Switch Configuration.
- Overwrite the settings on an existing distributed switch. See Restore a vSphere Distributed Switch Configuration.

You can also export, import, and restore only port group configurations. See Export, Import, and Restore vSphere Distributed Port Group Configurations.

Import a vSphere Distributed Switch Configuration

Import a stored configuration file to create a new vSphere Distributed Switch or to restore a switch that has been deleted earlier.

The configuration file contains the networking settings of the switch. By using it you can also replicate the switch in other virtual environments.

Note: You can use a saved configuration file to replicate the switch instance, its host associations, and policies. You cannot replicate the connection of physical NICs to uplink ports or ports on link aggregation groups.

1. In the vSphere Client, navigate to a data center.
2. Right-click the data center and select **Distributed Switch** > **Import Distributed Switch**.
3. Browse to the location of the configuration file.
4. To assign the keys from the configuration file to the switch and its port groups, select the **Preserve original distributed switch and port group identifiers** check box and click **Next**.

   You can use the **Preserve original distributed switch and port group identifiers** option in the following cases:

   - Recreate a deleted switch.
   - Restore a switch whose upgrade has failed.

   All port groups are recreated and the hosts that have been connected to the switch are added again.
5. Review the settings for the switch and click **Finish**.

A new distributed switch is created with settings from the configuration file. If you have included distributed port group information in the configuration file, the port groups are also created.

Restore a vSphere Distributed Switch Configuration

Use the restore option to reset the configuration of an existing distributed switch to the settings in the configuration file. Restoring a distributed switch changes the settings on the selected switch back to the settings saved in the configuration file.

Note: You can use a saved configuration file to restore policies and hosts associations on the distributed switch. You cannot restore the connection of physical NICs to uplink ports or ports of link aggregation groups.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch in the navigator and select **Settings** > **Restore Configuration**.
3. Browse for the configuration backup file to use.
4. Select **Restore distributed switch and all port groups** or **Restore distributed switch only** and click **Next**
5. Review the summary information for the restore.

   Restoring a distributed switch will overwrite the current settings of the distributed switch and its port groups. It will not delete existing port groups that are not part of the configuration file.
6. Click **Finish**.

   The distributed switch configuration has been restored to the settings in the configuration file.

Export, Import, and Restore vSphere Distributed Port Group Configurations

You can export vSphere distributed port group configurations to a file. The configuration file allows you to preserve valid port group configurations, enabling distribution of these configurations to other deployments.

You can export port group information at the same time you export distributed switch configurations. See Backing Up and Restoring a vSphere Distributed Switch Configuration.

Export vSphere Distributed Port Group Configurations

You can export a distributed port group configurations to a file. The configuration preserves valid network configurations, enabling distribution of these configurations to other deployments.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Right-click the distributed port group and select **Export Configuration**.
3. Optional: In the **Descriptions** field, type notes about this configuration.
4. Click **OK**.
   Click **Yes** to save the configuration file to your local system.

You now have a configuration file that contains all the settings for the selected distributed port group. You can use this file to create multiple copies of this configuration on an existing deployment, or overwrite settings of existing distributed port groups to conform to the selected settings.

You can use the exported configuration file to do the following tasks:

- To create a copy of the exported distributed port group, see Import a vSphere Distributed Port Group Configuration.
- To overwrite settings on an existing distributed port group, see Restore a vSphere Distributed Port Group Configuration.

Import a vSphere Distributed Port Group Configuration

Use import to create a distributed port group from a configuration file.

If an existing port group has the same name as the imported port group, the new port group name has a number appended in parentheses. The settings from the imported configuration are applied to the new port group and the settings of the original port group remain unchanged.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch and select **Distributed Port Group** > **Import Distributed Port Group**.
3. Browse to the location of your saved configuration file and click **Next**.
4. Review the import settings before completing the import.
5. Click **Finish.**

Restore a vSphere Distributed Port Group Configuration

Use the restore option to reset the configuration of an existing distributed port group to the settings in a configuration file.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Right-click the distributed port group and select **Restore Configuration**.
3. Select one of the following and click **Next**:
   - **Restore to previous configuration** to roll your port group configuration back one step. You cannot restore the port group configuration completely if you have performed more than one step.
   - **Restore configuration from a file** lets you restore the port group configuration from an exported backup file. You can also use a distributed switch backup file as long as it contains configuration information for the port group.
4. Review the summary information for the restore.

   The restore operation overwrites the current settings of the distributed port group with the settings from the backup. If you are restoring the port group configuration from a switch backup file, the restore operation does not delete existing port groups that are not a part of the file.
5. Click **Finish**.

Rollback and Recovery of the Management Network

You can prevent and recover from misconfiguration of the management network by using the rollback and recovery support of the vSphere Distributed Switch and vSphere Standard Switch.

Rollback is available for use on both standard and distributed switches. To fix invalid configuration of the management network, you can connect directly to a host to fix the issues through the DCUI.

vSphere Networking Rollback

By rolling configuration changes back, vSphere protects hosts from losing connection to vCenter Server as a result from misconfiguration of the management network.

In vSphere networking rollback is enabled by default. However, you can enable or disable rollbacks at the vCenter Server level.

Host Networking Rollbacks

Host networking rollbacks occur when an invalid change is made to the networking configuration for the connection with vCenter Server. Every network change that disconnects a host also triggers a rollback. The following examples of changes to the host networking configuration might trigger a rollback:

- Updating the speed or duplex of a physical NIC.
- Updating DNS and routing settings.
- Updating teaming and failover policies or traffic shaping policies of a standard port group that contains the management VMkernel network adapter.
- Updating the VLAN of a standard port group that contains the management VMkernel network adapter.
- Increasing the MTU of management VMkernel network adapter and its switch to values not supported by the physical infrastructure.
- Changing the IP settings of management VMkernel network adapters.
- Removing the management VMkernel network adapter from a standard or distributed switch.
- Removing a physical NIC of a standard or distributed switch containing the management VMkernel network adapter.
- Migrating the management VMkernel adapter from vSphere standard to distributed switch.

If a network disconnects for any of these reasons, the task fails and the host reverts to the last valid configuration.

vSphere Distributed Switch Rollbacks

Distributed switch rollbacks occur when invalid updates are made to distributed switches, distributed port groups, or distributed ports. The following changes to the distributed switch configuration trigger a rollback:

- Changing the MTU of a distributed switch.
- Changing the following settings in the distributed port group of the management VMkernel network adapter:
  - Teaming and failover
  - VLAN
  - Traffic shaping
- Blocking all ports in the distributed port group containing the management VMkernel network adapter.
- Overriding the policies on at the level of the distributed port for the management VMkernel network adapter.

If a configuration becomes invalid because of any of the changes, one or more hosts might become out of synchronization with the distributed switch.

If you know where the conflicting configuration setting is located, you can manually correct the setting. For example, if you have migrated a management VMkernel network adapter to a new VLAN, the VLAN might not be actually trunked on the physical switch. When you correct the physical switch configuration, the next distributed switch-to-host synchronization will resolve the configuration problem.

If you are not sure where the problem exists, you can restore the state of the distributed switch or distributed port group to an earlier configuration. See Restore a vSphere Distributed Port Group Configuration.

Disable Network Rollback

Rollback is enabled by default in vSphere. You can disable rollback in vCenter Server by using the vSphere Client.

1. In the vSphere Client, navigate to a vCenter Server instance.
2. On the **Configure** tab, expand **Settings** and select **Advanced Settings**.
3. Click **Edit Settings**.
4. Select the `config.vpxd.network.rollback` key, and change the value to false.
   If the key is not present, you can add it and set the value to false.

5. Click **OK**.
6. Restart vCenter Server to apply the changes.

Disable Network Rollback by Using the vCenter Server Configuration File

Rollback is enabled by default in vSphere. You can disable rollback by editing the `vpxd.cfg` configuration file of vCenter Server directly.

1. On the host machine of , navigate to the directory `/etc/vmware-vpx`.
2. Open the `vpxd.cfg` file for editing.
3. In the `<network>` element, set the `<rollback>` element to `false`:

```
<config>
 <vpxd>
  <network>
    <rollback>false</rollback>
  </network>
 </vpxd>
</config>
```

4. Save and close the file.
5. Restart the vCenter Server system.

Resolve Errors in the Management Network Configuration on a vSphere Distributed Switch

You can use the Direct Console User Interface (DCUI) to restore the connection between vCenter Server and a host that accesses the management network through a distributed switch.

Verify that the management network is configured on a port group on the distributed switch.

If networking rollback is disabled, misconfiguring the port group for the management network on the distributed switch leads to loss of connection between vCenter Server and the hosts that are added to the switch. You have to use the DCUI to connect each host individually.

If the uplinks that you use to restore the management network are also used by VMkernel adapters that handle other types of traffic (vMotion, Fault Tolerance, and so on), the adapters loose network connectivity after the restore.

For more information about accessing and using the DCUI, see the *vSphere Security* documentation.

Note: Recovery of the management connection on a distributed switch is not supported on stateless ESXi instances.

1. Connect to the DCUI of the host.
2. From the **Network Restore Options** menu, select **Restore vDS**.
3. Configure the uplinks and optionally the VLAN for the management network.
4. Apply the configuration.

The DCUI creates a local ephemeral port and applies the values you provided for the VLAN and uplinks. The DCUI moves the VMkernel adapter for the management network to the new local port to restore connectivity to vCenter Server.

After the connection of the host to vCenter Server is restored, correct the configuration of the distributed port group and re-add the VMkernel adapter to the group.

Networking Policies

Policies set at the standard switch or distributed port group level apply to all of the port groups on the standard switch or to ports in the distributed port group. The exceptions are the configuration options that are overridden at the standard port group or distributed port level.

Watch the video about applying networking policies on vSphere standard and distributed switches.

Applying Networking Policies on a vSphere Standard or Distributed Switch

You apply networking policies differently on vSphere Standard Switches and vSphere Distributed Switches. Not all policies that are available for a vSphere Distributed Switch are also available for a vSphere Standard Switch.

Table 181: Virtual Switch Objects Where Policies Apply

Virtual Switch	Virtual Switch Object	Description
vSphere Standard Switch	Entire switch	When you apply policies on the entire standard switch, the policies are propagated to all standard port groups on the switch.
	Standard port group	You can apply different policies on individual port groups by overriding the policies that are inherited from the switch.
vSphere Distributed Switch	Distributed port group	When you apply policies on a distributed port group, the policies are propagated to all ports in the group.
	Distributed port	You can apply different policies on individual distributed ports by overriding the policies that are inherited from the distributed port group.
	Uplink port group	You can apply policies at uplink port group level, and the are policies are propagated to all ports in the group.
	Uplink port	You can apply different policies on individual uplink ports by overriding the policies that are inherited from the uplink port group.

Table 182: Policies Available for a vSphere Standard Switch and vSphere Distributed Switch

Policy	Standard Switch	Distributed Switch	Description
Teaming and failover	Yes	Yes	Lets you configure the physical NICs that handle the network traffic for a standard switch, standard port group, distributed port group, or distributed port. You arrange the physical NICs in a failover order and apply different load balancing policies over them.
Security	Yes	Yes	Provides protection of traffic against MAC address impersonation and unwanted port scanning. The networking security policy is implemented in Layer 2 of the networking protocol stack.
Traffic shaping	Yes	Yes	Lets you restrict the network bandwidth that is available to ports, but also to allow bursts of traffic to flow through at higher speeds. ESXi shapes outbound network traffic on standard switches and inbound and outbound traffic on distributed switches.
VLAN	Yes	Yes	Lets you configure the VLAN tagging for a standard or distributed switch. You can configure External Switch Tagging(EST), Virtual Switch Tagging (VST), and Virtual Guest Tagging (VGT).

Policy	Standard Switch	Distributed Switch	Description
Monitoring	No	Yes	Enables and disables NetFlow monitoring on a distributed port or port group.
Traffic filtering and marking	No	Yes	Lest you protect the virtual network from unwanted traffic and security attacks or apply a QoS tag to a certain traffic type.
Resources allocation	No	Yes	Lets you associate a distributed port or port group with a user-defined network resource pool. In this way, you can better control the bandwidth that is available to the port or port group. You can use the resource allocation policy with vSphere Network I/O Control version 2 and 3.
Port blocking	No	Yes	Lets you selectively block ports from sending and receiving data.

Configure Overriding Networking Policies on Port Level

To apply different policies for distributed ports, you configure the per-port overriding of the policies that are set at the port group level. You can also enable the reset of any configuration that is set on per-port level when a distributed port disconnects from a virtual machine.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Right-click the distributed port group and select **Edit Settings**.
3. Select the **Advanced** page.

Option	Description
Configure reset at disconnect	From the drop-down menu, enable or disable reset at disconnect. When a distributed port is disconnected from a virtual machine, the configuration of the distributed port is reset to the distributed port group setting. Any per-port overrides are discarded.
Override port policies	Select the distributed port group policies to be overridden on a per-port level.

4. Optional: Use the policy pages to set overrides for each port policy.
5. Click **OK**.

Teaming and Failover Policy

NIC teaming lets you increase the network capacity of a virtual switch by including two or more physical NICs in a team. To determine how the traffic is rerouted in case of adapter failure, you include physical NICs in a failover order. To determine how the virtual switch distributes the network traffic between the physical NICs in a team, you select load balancing algorithms depending on the needs and capabilities of your environment.

NIC Teaming Policy

You can use NIC teaming to connect a virtual switch to multiple physical NICs on a host to increase the network bandwidth of the switch and to provide redundancy. A NIC team can distribute the traffic between its members and provide passive failover in case of adapter failure or network outage. You set NIC teaming policies at virtual switch or port group level for a vSphere Standard Switch and at a port group or port level for a vSphere Distributed Switch.

Note: All ports on the physical switch in the same team must be in the same Layer 2 broadcast domain.

Load Balancing Policy

The Load Balancing policy determines how network traffic is distributed between the network adapters in a NIC team. vSphere virtual switches load balance only the outgoing traffic. Incoming traffic is controlled by the load balancing policy on the physical switch.

For more information about each load balancing algorithm, see Load Balancing Algorithms Available for Virtual Switches.

Network Failure Detection Policy

You can specify one of the following methods that a virtual switch uses for failover detection.

Link status only	Relies only on the link status that the network adapter provides. Detects failures, such as removed cables and physical switch power failures. However, link status does not detect the following configuration errors: • Physical switch port that is blocked by spanning tree or is misconfigured to the wrong VLAN . • Pulled cable that connects a physical switch to another networking devices, for example, an upstream switch .
Beacon probing	Sends out and listens for Ethernet broadcast frames, or beacon probes, that physical NICs send to detect link failure in all physical NICs in a team. ESXi hosts send beacon packets every second. Beacon probing is most useful to detect failures in the closest physical switch to the ESXi host, where the failure does not cause a link-down event for the host. Use beacon probing with three or more NICs in a team because ESXi can detect failures of a single adapter. If only two NICs are assigned and one of them loses connectivity, the switch cannot determine which NIC needs to be taken out of service because both do not receive beacons and as a result all packets sent to both uplinks. Using at least three NICs in such a team allows for n-2 failures where n is the number of NICs in the team before reaching an ambiguous situation.

Failback Policy

By default, a failback policy is enabled on a NIC team. If a failed physical NIC returns online, the virtual switch sets the NIC back to active by replacing the standby NIC that took over its slot.

If the physical NIC that stands first in the failover order experiences intermittent failures, the failback policy might lead to frequent changes in the NIC that is used. The physical switch sees frequent changes in MAC addresses, and the physical switch port might not accept traffic immediately when an adapter becomes online. To minimize such delays, you might consider changing the following settings on the physical switch:

- Disable Spanning Tree Protocol (STP) on physical NICs that are connected to ESXi hosts .
- For Cisco based networks, enable PortFast mode for access interfaces or PortFast trunk mode for trunk interfaces. This might save about 30 seconds during the initialization of the physical switch port.
- Disable the trunking negotiation.

Notify Switches Policy

By using the notify switches policy, you can determine how the ESXi host communicates failover events. When a physical NIC connects to the virtual switch or when traffic is rerouted to a different physical NIC in the team, the virtual switch sends notifications over the network to update the lookup tables on physical switches. Notifying the physical switch offers lowest latency when a failover or a migration with vSphere vMotion occurs.

Related Links

Create a vSphere Standard Switch on page 2149

Create a vSphere Standard Switch to provide network connectivity for hosts, virtual machines, and to handle VMkernel traffic. Depending on the connection type that you want to create, you can create a new vSphere Standard Switch with a VMkernel adapter, only connect physical network adapters to the new switch, or create the switch with a virtual machine port group.

Load Balancing Algorithms Available for Virtual Switches

You can configure various load balancing algorithms on a virtual switch to determine how network traffic is distributed between the physical NICs in a team.

Route Based on Originating Virtual Port

The virtual switch selects uplinks based on the virtual machine port IDs on the vSphere Standard Switch or vSphere Distributed Switch.

Route Based on Originating Virtual Port is the default load balancing method on the vSphere Standard Switch and vSphere Distributed Switch.

Each virtual machine running on an ESXi host has an associated virtual port ID on the virtual switch. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine port ID and the number of uplinks in the NIC team. After the virtual switch selects an uplink for a virtual machine, it always forwards traffic through the same uplink for this virtual machine as long as the machine runs on the same port. The virtual switch calculates uplinks for virtual machines only once, unless uplinks are added or removed from the NIC team.

The port ID of a virtual machine is fixed while the virtual machine runs on the same host. If you migrate, power off, or delete the virtual machine, its port ID on the virtual switch becomes free. The virtual switch stops sending traffic to this port, which reduces the overall traffic for its associated uplink. If a virtual machine is powered on or migrated, it might appear on a different port and use the uplink, which is associated with the new port.

Table 183: Considerations on Using Route Based on Originating Virtual Port

Considerations	Description
Advantages	• An even distribution of traffic if the number virtual NICs is greater than the number of physical NICs in the team. • Low resource consumption, because in most cases the virtual switch calculates uplinks for virtual machines only once. • No changes on the physical switch are required.
Disadvantages	• The virtual switch is not aware of the traffic load on the uplinks and it does not load balance the traffic to uplinks that are less used. • The bandwidth that is available to a virtual machine is limited to the speed of the uplink that is associated with the relevant port ID, unless the virtual machine has more than one virtual NIC.

Related Links

Route Based on Source MAC Hash on page 2247

The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.

Route Based on IP Hash on page 2248

The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.

Route Based on Physical NIC Load on page 2249
Route Based on Physical NIC Load is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. It is only for vSphere Distributed Switch.

Use Explicit Failover Order on page 2250
No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order and that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.

Route Based on Source MAC Hash

The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.

Table 184: Considerations on Using Route Based on Source MAC Hash

Considerations	Description
Advantages	• A more even distribution of the traffic than Route Based on Originating Virtual Port, because the virtual switch calculates an uplink for every packet. • Virtual machines use the same uplink because the MAC address is static. Powering a virtual machine on or off does not change the uplink that the virtual machine uses. • No changes on the physical switch are required.
Disadvantages	• The bandwidth that is available to a virtual machine is limited to the speed of the uplink that is associated with the relevant port ID, unless the virtual machine uses multiple source MAC addresses. • Higher resource consumption than Route Based on Originating Virtual Port, because the virtual switch calculates an uplink for every packet. • The virtual switch is not aware of the load of the uplinks, so uplinks might become overloaded.

Related Links

Route Based on Originating Virtual Port on page 2246
The virtual switch selects uplinks based on the virtual machine port IDs on the vSphere Standard Switch or vSphere Distributed Switch.

Route Based on IP Hash on page 2248
The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.

Route Based on Physical NIC Load on page 2249
Route Based on Physical NIC Load is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. It is only for vSphere Distributed Switch.

Use Explicit Failover Order on page 2250
No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order and that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.

Route Based on IP Hash

The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.

To calculate an uplink for a virtual machine, the virtual switch takes the last octet of both source and destination IP addresses in the packet, puts them through a XOR operation, and then runs the result through another calculation based on the number of uplinks in the NIC team. The result is a number between 0 and the number of uplinks in the team minus one. For example if a NIC team has four uplinks, the result is a number between 0 and 3 as each number is associated with a NIC in the team. For non-IP packets, the virtual switch takes two 32-bit binary values from the frame or packet from where the IP address would be located.

Any virtual machine can use any uplink in the NIC team depending on the source and destination IP address. In this way, each virtual machine can use the bandwidth of any uplink in the team. If a virtual machine runs in an environment with a large number of independent virtual machines, the IP hash algorithm can provide an even spread of the traffic between the NICs in the team. When a virtual machine communicates with multiple destination IP addresses, the virtual switch can generate a different hash for each destination IP. In this way, packets can use different uplinks on the virtual switch that results in higher potential throughput.

However, if your environment has a small number of IP addresses, the virtual switch might consistently pass the traffic through one uplink in the team. For example, if you have a database server that is accessed by one application server, the virtual switch always calculates the same uplink, because only one source-destination pair exists.

Physical Switch Configuration

To ensure that IP hash load balancing works correctly, you must have an Etherchannel configured on the physical switch. An Etherchannel bonds multiple network adapters into a single logical link. When ports are bound into an Etherchannel, every time the physical switch receives a packet from the same virtual machine MAC address on different ports, the switch updates its content addressable memory (CAM) table correctly.

For example, if the physical switch receives packets on ports 01 and 02 from MAC address A, the switch makes a 01-A and a 02-A entry in its CAM table. As a result, the physical switch distributes the incoming traffic to the correct ports. Without an Etherchannel, the physical switch first makes a record that a packet from MAC address A is received on port 01, then updates the same record that a packet from MAC address A is received on port 02. Hence, the physical switch forwards incoming traffic only on port 02, and might result in packets not reaching their destination and overloading the corresponding uplink.

Limitations and Configuration Requirements

- ESXi hosts support IP hash teaming on a single physical switch or stacked switches.
- ESXi hosts support only 802.3ad link aggregation in Static mode . You can only use a static Etherchannel with vSphere Standard Switches. LACP is not supported. If you enable IP hash load balancing without 802.3ad link aggregation and the reverse, you might experience networking disruptions.
- You must use Link Status Only as network failure detection with IP hash load balancing.
- You must set all uplinks from the team in the Active failover list . The Standby and Unused lists must be empty.
- The number of ports in the Etherchannel must be same as the number of uplinks in the team.

Considerations on Using Route Based on IP Hash

Considerations	Description
Advantages	• A more even distribution of the load compared to Route Based on Originating Virtual Port and Route Based on Source MAC Hash, as the virtual switch calculates the uplink for every packet.

Considerations	Description
	• A potentially higher throughput for virtual machines that communicate with multiple IP addresses.
Disadvantages	• Highest resource consumption compared to the other load balancing algorithms. • The virtual switch is not aware of the actual load of the uplinks. • Requires changes on the physical network. • Complex to troubleshoot.

Related Links

Route Based on Originating Virtual Port on page 2246
The virtual switch selects uplinks based on the virtual machine port IDs on the vSphere Standard Switch or vSphere Distributed Switch.

Route Based on Source MAC Hash on page 2247
The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.

Route Based on Physical NIC Load on page 2249
Route Based on Physical NIC Load is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. It is only for vSphere Distributed Switch.

Use Explicit Failover Order on page 2250
No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order and that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.

Route Based on Physical NIC Load

Route Based on Physical NIC Load is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. It is only for vSphere Distributed Switch.

The distributed switch calculates uplinks for virtual machines by taking their port ID and the number of uplinks in the NIC team. The distributed switch tests the uplinks every 30 seconds, and if their load exceeds 75 percent of usage, the port ID of the virtual machine with the highest I/O is moved to a different uplink.

Table 185: Considerations on Using Route Based on Physical NIC Load

Considerations	Description
Advantages	• Low resource consumption because the distributed switch calculates uplinks for virtual machines only once and checking the load of uplinks has minimal impact. • The distributed switch is aware of the load of uplinks and takes care to reduce it if needed. • No changes on the physical switch are required.
Disadvantages	• The bandwidth that is available to virtual machines is limited to the uplinks that are connected to the distributed switch.

Related Links

Route Based on Originating Virtual Port on page 2246

The virtual switch selects uplinks based on the virtual machine port IDs on the vSphere Standard Switch or vSphere Distributed Switch.

Route Based on Source MAC Hash on page 2247
The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.

Route Based on IP Hash on page 2248
The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.

Use Explicit Failover Order on page 2250
No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order and that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.

Use Explicit Failover Order

No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order and that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.

Related Links

Route Based on Originating Virtual Port on page 2246
The virtual switch selects uplinks based on the virtual machine port IDs on the vSphere Standard Switch or vSphere Distributed Switch.

Route Based on Source MAC Hash on page 2247
The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.

Route Based on IP Hash on page 2248
The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.

Route Based on Physical NIC Load on page 2249
Route Based on Physical NIC Load is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. It is only for vSphere Distributed Switch.

Configure NIC Teaming, Failover, and Load Balancing on a vSphere Standard Switch or Standard Port Group

Include two or more physical NICs in a team to increase the network capacity of a vSphere Standard Switch or standard port group. Configure failover order to determine how network traffic is rerouted in case of adapter failure. Select a load balancing algorithm to determine how the standard switch distributes the traffic between the physical NICs in a team.

Configure NIC teaming, failover, and load balancing depending on the network configuration on the physical switch and the topology of the standard switch. See Teaming and Failover Policy and Load Balancing Algorithms Available for Virtual Switches for more information.

If you configure the teaming and failover policy on a standard switch, the policy is propagated to all port groups in the switch. If you configure the policy on a standard port group, it overrides the policy inherited from the switch.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Navigate to the Teaming and Failover policy for the standard switch, or standard port group.

Option	Action
Standard Switch	1. Select the switch from the list. 2. Click **Edit settings** and select **Teaming and failover**.
Standard port group	1. Select the switch where the port group resides. 2. From the switch topology diagram, select the standard port group and click **Edit settings**. 3. Select **Teaming and failover**. 4. Select **Override** next to the policies that you want to override.

4. From the **Load balancing** drop-down menu, specify how the virtual switch load balances the outgoing traffic between the physical NICs in a team.

Option	Description
Route based on the originating virtual port	Select an uplink based on the virtual port IDs on the switch. After the virtual switch selects an uplink for a virtual machine or a VMkernel adapter, it always forwards traffic through the same uplink for this virtual machine or VMkernel adapter.
Route based on IP hash	Select an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, the switch uses the data at those fields to compute the hash . IP-based teaming requires that the physical switch is configured with EtherChannel.
Route based on source MAC hash	Select an uplink based on a hash of the source Ethernet.
Use explicit failover order	From the list of active adapters, always use the highest order uplink that passes failover detection criteria. No actual load balancing is performed with this option.

5. From the **Network failure detection** drop-down menu, select the method that the virtual switch uses for failover detection.

Option	Description
Link status only	Relies only on the link status that the network adapter provides. This option detects failures such as removed cables and physical switch power failures.
Beacon probing	Sends out and listens for beacon probes on all NICs in the team, and uses this information, in addition to link status, to determine link failure. sends beacon packets every second. The NICs must be in an active/active or active/standby configuration because the NICs in an unused state do not participate in beacon probing.

6. From the **Notify switches** drop-down menu, select whether the standard or distributed switch notifies the physical switch in case of a failover.

   Note: If the **Notify switches** is set to **Yes**, then all the connected ports, port groups, and distributed switches are connected back to the host when vCenter Server reconnects with ESXi hosts.

   Note: Set this option to **No** if a connected virtual machine is using Microsoft Network Load Balancing in unicast mode. No issues exist with Network Load Balancing running in multicast mode.

7.

8. From the **Failback** drop-down menu, select whether a physical adapter is returned to active status after recovering from a failure.

   If failback is set to **Yes**, the default selection, the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any.

   If failback is set to **No** for a standard port, a failed adapter is left inactive after recovery until another currently active adapter fails and must be replaced.

9. Specify how the uplinks in a team are used when a failover occurs by configuring the Failover Order list.

   If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, use the up and down arrow keys to move uplinks into different groups.

Option	Description
Active adapters	Continue to use the uplink if the network adapter connectivity is up and active.
Standby adapters	Use this uplink if one of the active physical adapter is down.
Unused adapters	Do not use this uplink.

10. Click **OK**.

Configure NIC Teaming, Failover, and Load Balancing on a Distributed Port Group or Distributed Port

Include two or more physical NICs in a team to increase the network capacity of a distributed port group or port. Configure failover order to determine how network traffic is rerouted in case of adapter failure. Select a load balancing algorithm to determine how the distributed switch load balances the traffic between the physical NICs in a team.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

Configure NIC teaming, failover, and load balancing according with the network configuration on the physical switch and the topology of the distributed switch. See Teaming and Failover Policy and Load Balancing Algorithms Available for Virtual Switches for more information.

If you configure the teaming and failover policy for a distributed port group, the policy is propagated to all ports in the group. If you configure the policy for a distributed port, it overrides the policy inherited from the group.

Note: Setting failback option is not supported with **Route based on physical NIC load** teaming policy.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Navigate the Teaming and Failover policy on the distributed port group or port.

Option	Action
Distributed port group	1. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**. 2. Select the port group and click **Next**.

Option	Action
	3. Select **Teaming and failover**.
Distributed port	1. On the **Networks** tab, click **Distributed Port Groups** and double-click a distributed port group. 2. On the **Ports** tab, select a port and click **Edit distributed port settings**. 3. Select **Teaming and failover**. 4. Select **Override** next to the properties that you want to override.

3. From the **Load balancing** drop-down menu, specify how the virtual switch load balances the outgoing traffic between the physical NICs in a team.

Option	Description
Route based on the originating virtual port	Select an uplink based on the virtual port IDs on the switch. After the virtual switch selects an uplink for a virtual machine or a VMkernel adapter, it always forwards traffic through the same uplink for this virtual machine or VMkernel adapter.
Route based on IP hash	Select an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, the switch uses the data at those fields to compute the hash . IP-based teaming requires that the physical switch is configured with EtherChannel.
Route based on source MAC hash	Select an uplink based on a hash of the source Ethernet.
Route based on physical NIC load	Available for distributed port groups or distributed ports. Select an uplink based on the current load of the physical network adapters connected to the port group or port. If an uplink remains busy at 75 percent or higher for 30 seconds, the host proxy switch moves a part of the virtual machine traffic to a physical adapter that has free capacity. **Note:** Selecting **Route based on physical NIC load** prevents you from setting a failback option for a distributed port group.
Use explicit failover order	From the list of active adapters, always use the highest order uplink that passes failover detection criteria. No actual load balancing is performed with this option.

4. From the **Network failure detection** drop-down menu, select the method that the virtual switch uses for failover detection.

Option	Description
Link status only	Relies only on the link status that the network adapter provides. This option detects failures such as removed cables and physical switch power failures.
Beacon probing	Sends out and listens for beacon probes on all NICs in the team, and uses this information, in addition to link status, to determine link failure. sends beacon packets every second. The NICs must be in an active/active or active/standby configuration because the NICs in an unused state do not participate in beacon probing.

5. From the **Notify switches** drop-down menu, select whether the standard or distributed switch notifies the physical switch in case of a failover.

   Note: If the **Notify switches** is set to **Yes**, then all the connected ports, port groups, and distributed switches are connected back to the host when vCenter Server reconnects with ESXi hosts.

   Note: Set this option to **No** if a connected virtual machine is using Microsoft Network Load Balancing in unicast mode. No issues exist with Network Load Balancing running in multicast mode.

6. From the **Failback** drop-down menu, select whether a physical adapter is returned to active status after recovering from a failure.

   If failback is set to **Yes**, the default selection, the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any.

   If failback is set to **No** for a distributed port, a failed adapter is left inactive after recovery only if the associated virtual machine is running. When the **Failback** option is **No** and a virtual machine is powered off, if all active physical adapters fail and then one of them recovers, the virtual NIC is connected to the recovered adapter instead of to a standby one after the virtual machine is powered on. Powering a virtual machine off and then on leads to reconnecting the virtual NIC to a distributed port. The distributed switch considers the port as newly added, and assigns it the default uplink port, that is, the active uplink adapter.

7. Specify how the uplinks in a team are used when a failover occurs by configuring the Failover Order list.

   If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, use the up and down arrow keys to move uplinks into different groups.

Option	Description
Active adapters	Continue to use the uplink if the network adapter connectivity is up and active.
Standby adapters	Use this uplink if one of the active physical adapter is down.
Unused adapters	Do not use this uplink.

8. Review your settings and apply the configuration.

VLAN Policy

VLAN policies determine how VLANs function across your network environment.

A virtual local area network (VLAN) is a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if not on the same network switch.

The scope of VLAN policies can be distributed port groups and ports, and uplink port groups and ports.

Configure VLAN Tagging on a Distributed Port Group or Distributed Port

To apply VLAN tagging globally on all distributed ports, you must set the VLAN policy on a distributed port group. To integrate the virtual traffic on the port with physical VLANs in a different way from the parent distributed port group, you must use the VLAN policy on a distributed port.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Navigate to the VLAN policy on the distributed port group or distributed port.

Option	Action
Distributed port group	1. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**. 2. Select **VLAN** and click **Next**. 3. Select the port group and click **Next**.
Distributed port	1. On the **Networks** tab, click **Distributed Port Groups** and double-click a distributed port group. 2. On the **Ports** tab, select a port and click the **Edit distributed port settings** icon. 3. Select **VLAN**. 4. Select **Override** next to the properties to override.

3. From the **VLAN type** drop-down menu, select the type of VLAN traffic filtering and marking, and click **Next**.

Option	Description
None	Do not use VLAN. Use this option in case of External Switch Tagging.
VLAN	Tag traffic with the ID from the **VLAN ID** field. Type a number between 1 and 4094 for Virtual Switch Tagging.
VLAN Trunking	Pass VLAN traffic with ID within the **VLAN trunk range** to guest operating system. You can set multiple ranges and individual VLANs by using a comma-separated list. For example: `1702-1705, 1848-1849`. Use this option for Virtual Guest Tagging.
Private VLAN	Associate the traffic with a private VLAN created on the distributed switch.

4. Review your settings and apply the configuration.

Related Links

VLAN Configuration on page 2281
Virtual LANs (VLANs) enable a single physical LAN segment to be further isolated so that groups of ports are isolated from one another as if they were on physically different segments.

Create a Private VLAN on page 2283
Create the necessary private VLANs on the vSphere Distributed Switch to be able to assign distributed ports to participate to a private VLAN.

Configure VLAN Tagging on an Uplink Port Group or Uplink Port

To configure VLAN traffic processing generally for all member uplinks, you must set the VLAN policy on an uplink port. To handle VLAN traffic through the port in a different way than for the parent uplink port group, you must set the VLAN policy on an uplink .

To override the VLAN policy at the port level, enable the port-level overrides. See Configure Overriding Networking Policies on Port Level.

Use the VLAN policy at the uplink port level to propagate a trunk range of VLAN IDs to the physical network adapters for traffic filtering. The physical network adapters drop the packets from the other VLANs if the adapters support filtering by VLAN. Setting a trunk range improves networking performance because physical network adapters filter traffic instead of the uplink ports in the group.

If you have a physical network adapter that does not support VLAN filtering, the VLANs still might not be blocked. In this case, configure VLAN filtering on a distributed port group or on a distributed port.

For information about VLAN filtering support, see the technical documentation from the adapter vendors.

1. In the vSphere Client, navigate to a distributed switch.
2. On the **Networks** tab, click **Uplink Port Groups**.
3. Navigate to the VLAN policy is on the uplink port group or port.

Option	Action
Uplink port group	1. Right-click an uplink port group in the list and select **Edit Settings**. 2. Click **VLAN**.
Uplink port	1. Double-click an uplink port group. 2. On the **Ports** tab, select a port and click the **Edit distributed port settings** tab. 3. Click **VLAN** and select **Override**.

4. Enter a **VLAN trunk range** value to propagate to the physical network adapters.
   For trunking of several ranges and individual VLANs, separate the entries with commas.
5. Click **OK**.

Security Policy

Networking security policy provides protection of traffic against MAC address impersonation and unwanted port scanning

The security policy of a standard or distributed switch is implemented in Layer 2 (Data Link Layer) of the network protocol stack. The three elements of the security policy are promiscuous mode, MAC address changes, and forged transmits. See the *vSphere Security* documentation for information about potential networking threats.

Configure the Security Policy for a vSphere Standard Switch or Standard Port Group

For a vSphere standard switch, you can configure the security policy to reject MAC address and promiscuous mode changes in the guest operating system of a virtual machine. You can override the security policy that is inherited from the standard switch on individual port groups.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Navigate to the Security policy for the standard switch or port group.

Option	Action
vSphere Standard Switch	1. Select a standard switch from the list. 2. Click **Edit settings**. 3. Select **Security**.
Standard port group	1. Select the standard switch where the port group resides. 2. In the topology diagram, select a standard port group. 3. Click **Edit settings**.

Option	Action
	4. Select **Security** and select **Override** next to the options to override.

4. Reject or accept promiscuous mode activation or MAC address changes in the guest operating system of the virtual machines attached to the standard switch or port group.

Option	Description
Promiscuous mode	• **Reject**. The VM network adapter receives only frames that are addressed to the virtual machine. • **Accept**.The virtual switch forwards all frames to the virtual machine in compliance with the active VLAN policy for the port to which the VM network adapter is connected. **Note:** Promiscuous mode is insecure mode of operation. Firewalls, port scanners, intrusion detection systems, must run in promiscuous mode.
MAC address changes	• **Reject**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter (set in the `.vmx` configuration file), the switch drops all inbound frames to the adapter. If the guest OS changes the effective MAC address of the virtual machine back to the MAC address of the VM network adapter, the virtual machine receives frames again. • **Accept**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter, the switch allows frames to the new address to pass.
Forged transmits	• **Reject**. The switch drops any outbound frame from a virtual machine adapter with a source MAC address that is different from the one in the `.vmx` configuration file. • **Accept**. The switch does not perform filtering, and permits all outbound frames.

5. Click **OK**.

Configure the Security Policy for a Distributed Port Group or Distributed Port

Set a security policy on a distributed port group to allow or reject promiscuous mode and MAC address changes from the guest operating system of the virtual machines associated with the port group. You can override the security policy inherited from the distributed port groups on individual ports.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Navigate to the Security policy for the distributed port group or port.

Option	Action
Distributed port group	1. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**. 2. Select **Security** and click **Next**. 3. Select the port group and click **Next**.
Distributed port	1. On the **Networks** tab, click **Distributed Port Groups** and double-click a distributed port group .

Option	Action
	2. On the **Ports** tab, select a port and click the **Edit settings** icon. 3. Select **Security**. 4. Select **Override** next to the properties to override.

3. Reject or accept promiscuous mode activation or MAC address changes in the guest operating system of the virtual machines attached to the distributed port group or port.

Option	Description
Promiscuous mode	• **Reject**. The VM network adapter receives only frames that are addressed to the virtual machine. • **Accept**.The virtual switch forwards all frames to the virtual machine in compliance with the active VLAN policy for the port to which the VM network adapter is connected. **Note:** Promiscuous mode is insecure mode of operation. Firewalls, port scanners, intrusion detection systems, must run in promiscuous mode.
MAC address changes	• **Reject**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter (set in the `.vmx` configuration file), the switch drops all inbound frames to the adapter. If the guest OS changes the effective MAC address of the virtual machine back to the MAC address of the VM network adapter, the virtual machine receives frames again. • **Accept**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter, the switch allows frames to the new address to pass.
Forged transmits	• **Reject**. The switch drops any outbound frame from a virtual machine adapter with a source MAC address that is different from the one in the `.vmx` configuration file. • **Accept**. The switch does not perform filtering, and permits all outbound frames.

4. Review your settings and apply the configuration.

Traffic Shaping Policy

A traffic shaping policy is defined by average bandwidth, peak bandwidth, and burst size. You can establish a traffic shaping policy for each port group and each distributed port or distributed port group.

ESXi shapes outbound network traffic on standard switches and inbound and outbound traffic on distributed switches. Traffic shaping restricts the network bandwidth available on a port, but can also be configured to allow bursts of traffic to flow through at higher speeds.

Average Bandwidth	Establishes the number of bits per second to allow across a port, averaged over time. This number is the allowed average load.
Peak Bandwidth	Maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This number limits the bandwidth that a port uses when it is using its burst bonus.
Burst Size	Maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus if it does not use all its allocated bandwidth. When the port needs more bandwidth than specified by the average bandwidth, it might be allowed to

temporarily transmit data at a higher speed if a burst bonus is available. This parameter limits the number of bytes that have accumulated in the burst bonus and transfers traffic at a higher speed.

Configure Traffic Shaping for a vSphere Standard Switch or Standard Port Group

ESXi lets you shape outbound traffic on standard switches or port groups. The traffic shaper restricts the network bandwidth available to any port, but you can also configure it to temporarily allow bursts of traffic to flow through a port at higher speeds.

The traffic shaping policies that you set at switch or port group level are applied at each individual port that participates in the switch or port group. For example, if you set an average bandwidth of 100000 Kbps on a standard port group, 100000 Kbps averaged over time can pass through each port that is associated with the standard port group.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Navigate to the traffic shaping policy on the standard switch or port group.

Option	Action
vSphere Standard Switch	1. Select a standard switch from the list. 2. Click **Edit settings**. 3. Select **Traffic shaping**.
Standard port group	1. Select the standard switch where the port group resides. 2. In the topology diagram, select a standard port group. 3. Click **Edit settings**. 4. Select **Traffic shaping** and select **Override** next to the options to override.

4. Configure traffic shaping policies.

Option	Description
Status	Enables setting limits on the amount of networking bandwidth allocated for each port that is associated with the standard switch or port group.
Average Bandwidth	Establishes the number of bits per second to allow across a port, averaged over time (the allowed average load).
Peak Bandwidth	The maximum number of bits per second to allow across a port when it is sending a burst of traffic. This setting tops the bandwidth used by a port whenever it is using its burst bonus. This parameter can never be smaller than the average bandwidth.
Burst Size	The maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than the average bandwidth specifies, the port can temporarily transmit data at a higher speed if a burst bonus is available. This parameter tops the number of bytes that can accumulate in the burst bonus and can be transferred at a higher speed.

5. For each traffic shaping policy (**Average Bandwidth**, **Peak Bandwidth**, and **Burst Size**), enter a bandwidth value.
6. Click **OK**.

Edit the Traffic Shaping Policy on a Distributed Port Group or Distributed Port

You can shape both inbound and outbound traffic on vSphere distributed port groups or distributed ports. The traffic shaper restricts the network bandwidth for any port in the group, but might also be configured to temporarily allow “bursts” of traffic to flow through a port at higher speeds.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

The traffic shaping policies that you set at distributed port group level are applied on each individual port that participates in the port group. For example, if you set an average bandwidth of 100000 Kbps on a distributed port group, 100000 Kbps averaged over time can pass through each port that is associated with the distributed port group.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Navigate to the Traffic Shaping policy for the distributed port group or port.

Option	Action
Distributed port group	1. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**. 2. Select **Traffic shaping** and click **Next**. 3. Select the port group and click **Next**.
Distributed port	1. On the **Networks** tab, click **Distributed Port Groups** and double-click a distributed port group . 2. On the **Ports** tab, select a port and click the **Edit distributed port settings** icon. 3. Select **Traffic shaping**. 4. Select **Override** next to the properties to override.

3. Configure traffic shaping policies.

   Note: The traffic is classified to ingress and egress according to the traffic direction in the switch, not in the host.

Option	Description
Status	Enable either **Ingress traffic shaping** or **Egress traffic shaping** by using the **Status** drop-down menus.
Average Bandwidth	Establishes the number of bits per second to allow across a port, averaged over time, that is, the allowed average load.
Peak Bandwidth	The maximum number of bits per second to allow across a port when it is sending/sending or receiving a burst of traffic. This parameter tops the bandwidth used by a port whenever it is using its burst bonus.
Burst Size	The maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than the average bandwidth specifies, the port can temporarily transmit data at a higher speed if a burst bonus is available. This parameter tops the number of bytes that might accumulate in the burst bonus and be transferred at a higher speed.

4. Review your settings and apply the configuration.

Resource Allocation Policy

The Resource Allocation policy allows you to associate a distributed port or port group with a user-created network resource pool. This policy provides you with greater control over the bandwidth given to the port or port group.

For information about creating and configuring network resource pools, see vSphere Network I/O Control.

Edit the Resource Allocation Policy on a Distributed Port Group

Associate a distributed port group with a network resource pool to give you greater control over the bandwidth that is given to the distributed port group.

- Enable Network I/O Control on the distributed switch. See Enable Network I/O Control on a vSphere Distributed Switch.
- Create and configure network resource pools. See Create a Network Resource Pool.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch in the navigator and select **Distributed Port Groups** > **Manage Distributed Port Groups**.
3. Select the **Resource allocation** check box and click **Next**.
4. Select the distributed port group to configure and click **Next**.
5. Add or remove the distributed port group from the network resource pool and click **Next**.
   - To add the distributed port group, select a user-defined resource pool from the **Network resource pool** drop-down menu.
   - To remove the distributed port group, select **default** from the **Network resource pool** drop-down menu.
6. Review your settings in the **Ready to complete** section and click **Finish**.
   Use the **Back** button to change any settings.

Monitoring Policy

The monitoring policy enables or disables NetFlow monitoring on a distributed port or port group.

NetFlow settings are configured at the vSphere distributed switch level. See Configure the NetFlow Settings of a vSphere Distributed Switch.

Manage NetFlow Monitoring on a Distributed Port Group or Distributed Port

You can configure NetFlow to monitor IP packets that are passing through the ports of a distributed port group or through individual distributed ports.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

You configure the NetFlow settings on the vSphere Distributed Switch. See Configure the NetFlow Settings of a vSphere Distributed Switch

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Navigate to the monitoring policy for the distributed port group or distributed port.

Option	Action
Distributed port group	1. From the **Actions** menu, select **Distributed Port Group** > **Manage Distributed Port Groups**. 2. Select **Monitoring** and click **Next**.

Option	Action
	3. Select the port group and click **Next**.
Distributed port	1. On the **Networks** tab, click **Distributed Port Groups** and double-click a distributed port group. 2. On the **Ports** tab, select a port and click the **Edit distributed port settings** icon. 3. Select **Monitoring**. 4. Select **Override** next to the properties to override.

3. From the **NetFlow** drop-down menu, select **Enabled** or **Disabled**, and click **Next**.
4. Verify your settings and apply the configuration.

Traffic Filtering and Marking Policy

In a vSphere distributed switch, by using the traffic filtering and marking policy, you can protect the virtual network from unwanted traffic and security attacks or apply a QoS tag to a certain type of traffic.

The traffic filtering and marking policy represents an ordered set of network traffic rules for security and for QoS tagging of the data flow through the ports of a distributed switch. In general, a rule consists of a qualifier for traffic, and of an action for restricting or prioritizing the matching traffic.

The vSphere distributed switch applies rules on traffic at different places in the data stream. The distributed switch applies traffic filter rules on the data path between the virtual machine network adapter and distributed port, or between the uplink port and physical network adapter for rules on uplinks.

Traffic Filtering and Marking on a Distributed Port Group or Uplink Port Group

Set traffic rules at the level of distributed port groups or of uplink port groups to introduce filtering and priority tagging for traffic access over virtual machines, VMkernel adapters, or physical adapters.

Enable Traffic Filtering and Marking on a Distributed Port Group or Uplink Port Group

Enable the traffic filtering and marking policy on a port group if you want to configure traffic security and marking on all virtual machine network adapters or uplink adapters that are participating in the group.

Note: You can disable the traffic filtering and marking policy on a particular port to avoid processing the traffic flowing through the port. See Disable Traffic Filtering and Marking on a Distributed Port or Uplink Port.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. Click the **Enable and reorder** button.
5. Click **Enable all traffic rules**.
6. Click **OK**.

Set up traffic marking or filtering on the data that is flowing through the ports of the distributed port group or through the uplink port group. See Mark Traffic on a Distributed Port Group or Uplink Port Group and Filter Traffic on a Distributed Port Group or Uplink Port Group.

Mark Traffic on a Distributed Port Group or Uplink Port Group

Assign priority tags to traffic, such as VoIP and streaming video, that has higher networking requirements for bandwidth, low latency, and so on. You can mark the traffic with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Priority tagging is a mechanism to mark traffic that has higher QoS demands. In this way, the network can recognize different classes of traffic. The network devices can handle the traffic from each class according to its priority and requirements.

You can also re-tag traffic to either raise or lower the importance of the flow. By using a low QoS tag, you can restrict data tagged in a guest operating system.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. If traffic filtering and marking is disabled, click **Enable and reorder** > **Enable all traffic rules** > **OK**.
5. Click **Add** to create a new rule, or select a rule and click **Edit** to edit it.
6. In the network traffic rule dialog box, select the **Tag** option from the **Action** drop-down menu.
7. Set the priority tag for the traffic within the scope of the rule.

Option	Description
CoS value	Mark the traffic matching the rule with a CoS priority tag in network Layer 2. Select the check box and type a value from 0 to 7.
DSCP value	Mark the traffic associated with the rule with a DSCP tag in network Layer 3. Select the check box and type a value from 0 to 63.

8. Specify the kind of traffic that the rule is applicable to.

   To determine if a data flow is in the scope of a rule for marking or filtering, the vSphere distributed switch examines the direction of the traffic, and properties like source and destination, VLAN, next level protocol, infrastructure traffic type, and so on.

   a) From the **Traffic direction** drop-down menu, select whether the traffic must be ingress, egress, or both so that the rule recognizes it as matching.

      The direction also influences how you are going to identify the traffic source and destination.

   b) By using qualifiers for system data type, Layer 2 packet attributes, and Layer 3 packet attributes set the properties that packets must have to match the rule.

      A qualifier represents a set of matching criteria related to a networking layer. You can match traffic to system data type, Layer 2 traffic properties, and Layer 3 traffic properties. You can use the qualifier for a specific networking layer or can combine qualifiers to match packets more precisely.

      - Use the system traffic qualifier to match packets to the type of virtual infrastructure data that is flowing through the ports of the group . For example, you can select NFS for data transfers to network storage.
      - Use the MAC traffic qualifier to match packets by MAC address, VLAN ID, and next level protocol.
        Locating traffic with a VLAN ID on a distributed port group works with Virtual Guest Tagging (VGT). To match traffic to VLAN ID if Virtual Switch Tagging (VST) is active, use a rule on an uplink port group or uplink port.
      - Use the IP traffic qualifier to match packets by IP version, IP address, and next level protocol and port.

9. In the rule dialog box, click **OK** to save the rule.

Voice over IP Traffic Marking

Voice over IP (VoIP) flows have special requirements for QoS in terms of low loss and delay. The traffic related to the Session Initiation Protocol (SIP) for VoIP usually has a DSCP tag equal to 26, which stands for Assured Forwarding Class 3 with Low Drop Probability (AF31).

For example, to mark outgoing SIP UDP packets to a subnet 192.168.2.0/24, you can use the following rule:

Rule Parameter	Parameter Value
Action	Tag
DSCP value	26
Traffic direction	Egress
Traffic qualifiers	IP Qualifier
Protocol	UDP
Destination port	5060
Source address	IP address matches 192.168.2.0 with prefix length 24

Related Links

System Traffic Qualifier on page 2273

By using the system traffic qualifier in a rule for port group or port, you can determine whether certain system data traffic must be marked with a QoS tag, allowed, or dropped.

MAC Traffic Qualifier on page 2274

By using the MAC traffic qualifier in a rule, you can define matching criteria for the Layer 2 (Data Link Layer) properties of packets such as MAC address, VLAN ID, and next level protocol that consumes the frame payload.

IP Traffic Qualifier on page 2275

By using the IP traffic qualifier in a rule, you can define criteria for matching traffic to the Layer 3 (Network Layer) properties such as IP version, IP address, next level protocol, and port.

Filter Traffic on a Distributed Port Group or Uplink Port Group

Allow or stop traffic for securing the data that flows through the ports of a distributed port group or uplink port group.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. If traffic filtering and marking is disabled, click **Enable and reorder** > **Enable all traffic rules** > **OK**.
5. Click **Add** to create a new rule, or select a rule and click **Edit** to edit it.
6. In the network traffic rule dialog box, use the Action options to let traffic pass through the ports of the distributed port group or uplink port group, or to restrict it.
7. Specify the kind of traffic that the rule is applicable to.

   To determine if a data flow is in the scope of a rule for marking or filtering, the vSphere distributed switch examines the direction of the traffic, and properties like source and destination, VLAN, next level protocol, infrastructure traffic type, and so on.
   a) From the **Traffic direction** drop-down menu, select whether the traffic must be ingress, egress, or both so that the rule recognizes it as matching.

      The direction also influences how you are going to identify the traffic source and destination.
   b) By using qualifiers for system data type, Layer 2 packet attributes, and Layer 3 packet attributes set the properties that packets must have to match the rule.

      A qualifier represents a set of matching criteria related to a networking layer. You can match traffic to system data type, Layer 2 traffic properties, and Layer 3 traffic properties. You can use the qualifier for a specific networking layer or can combine qualifiers to match packets more precisely.

      - Use the system traffic qualifier to match packets to the type of virtual infrastructure data that is flowing through the ports of the group . For example, you can select NFS for data transfers to network storage.
      - Use the MAC traffic qualifier to match packets by MAC address, VLAN ID, and next level protocol.
        Locating traffic with a VLAN ID on a distributed port group works with Virtual Guest Tagging (VGT). To match traffic to VLAN ID if Virtual Switch Tagging (VST) is active, use a rule on an uplink port group or uplink port.
      - Use the IP traffic qualifier to match packets by IP version, IP address, and next level protocol and port.
8. In the rule dialog box, click **OK** to save the rule.

Related Links

System Traffic Qualifier on page 2273
By using the system traffic qualifier in a rule for port group or port, you can determine whether certain system data traffic must be marked with a QoS tag, allowed, or dropped.

MAC Traffic Qualifier on page 2274
By using the MAC traffic qualifier in a rule, you can define matching criteria for the Layer 2 (Data Link Layer) properties of packets such as MAC address, VLAN ID, and next level protocol that consumes the frame payload.

IP Traffic Qualifier on page 2275
By using the IP traffic qualifier in a rule, you can define criteria for matching traffic to the Layer 3 (Network Layer) properties such as IP version, IP address, next level protocol, and port.

Working with Network Traffic Rules on a Distributed Port Group or Uplink Port Group

Define traffic rules in a distributed port group or uplink port group to introduce a policy for processing traffic related to virtual machines or to physical adapters. You can filter specific traffic or describe its QoS demands.

Note: You can override the rules of the policy for traffic filtering and marking at port level. See Working with Network Traffic Rules on a Distributed Port or Uplink Port.

View Traffic Rules on a Distributed Port Group or Uplink Group

View the traffic rules that form the traffic filtering and marking policy of a distributed port group or uplink port group.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. If traffic filtering and marking is disabled, click **Enable and reorder** > **Enable all traffic rules** > **OK**.
5. Examine **Action** to see if the rule filters traffic (Allow or Drop) or marks traffic (Tag) with special QoS demands.
6. From the upper list, select the rule for which you want to view the criteria for locating traffic.
   The traffic qualifying parameters of the rule appear in the Traffic Qualifiers list.

Edit a Traffic Rule on a Distributed Port Group or Uplink Port Group

Create or edit traffic rules, and use their parameters to configure a policy for filtering or marking the traffic on a distributed port group or uplink port group.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. If traffic filtering and marking is disabled, click **Enable and reorder** > **Enable all traffic rules** > **OK**.
5. Click **Add** to create a new rule, or select a rule and click **Edit** to edit it.

Name the network traffic rule, and deny, allow, or tag the target traffic.

Related Links

Mark Traffic on a Distributed Port Group or Uplink Port Group on page 2263
Assign priority tags to traffic, such as VoIP and streaming video, that has higher networking requirements for bandwidth, low latency, and so on. You can mark the traffic with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port Group or Uplink Port Group on page 2265
Allow or stop traffic for securing the data that flows through the ports of a distributed port group or uplink port group.

Change Rule Priorities on a Distributed Port Group or Uplink Port Group

Reorder the rules that form the traffic filtering and marking policy of a distributed port group or uplink port group to change the sequence of actions for processing traffic.

The vSphere distributed switch applies network traffic rules in a strict order. If a packet already satisfies a rule, the packet might not be passed to the next rule in the policy.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. Click the **Enable and reorder** button.
5. If traffic filtering and marking is disabled, click **Enable all traffic rules** to enable it.
6. Select a rule and use the **Move up** or **Move down** button to change its priority.
7. Click **OK** to apply the changes.

Delete a Traffic Rule on a Distributed Port Group or Uplink Port Group

Delete a traffic rule on a distributed port group or uplink port group to stop processing packets flowing to virtual machines or physical adapters in a specific way.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. If traffic filtering and marking is disabled, click **Enable and reorder** > **Enable all traffic rules** > **OK**.
5. Select the rule and click the**Delete** button.
6. Click **OK**.

Disable Traffic Filtering and Marking on a Distributed Port Group or Uplink Port Group

Let traffic flow to virtual machines or physical adapters without additional control related to security or QoS by disabling the traffic filtering and marking policy.

Note: You can enable and set up the traffic filtering and marking policy on a particular port. See Enable Traffic Filtering and Marking on a Distributed Port or Uplink Port.

1. Locate a distributed port group or an uplink port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups** to see the list of distributed port groups, or click **Uplink Port Groups** to see the list of uplink port groups.
2. Click a distributed port group or an uplink port group and select the **Configure** tab.
3. Under Settings, select **Traffic Filtering And Marking**.
4. Click the **Enable and reorder** button.
5. Use the toggle button to disable all traffic rules.
6. Click **OK**.

Traffic Filtering and Marking on a Distributed Port or Uplink Port

Filter traffic or describe its QoS demands for an individual virtual machine, VMkernel adapter, or physical adapter by configuring the traffic filtering and marking policy on a distributed port or uplink port.

Enable Traffic Filtering and Marking on a Distributed Port or Uplink Port

Enable the traffic filtering and marking policy on a port to configure traffic security and marking on a virtual machine network adapter, VMkernel adapter, or uplink adapter.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.
2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. Click the **Enable and reorder** button.
5. Use the toggle button to override the default settings.
6. Optional: Click **Enable all traffic rules**.

   If traffic rules are enabled on group level, after you override the default settings for the port, the traffic rules are automatically enabled.
7. Click **OK**.

Set up traffic filtering or marking for the data flowing through the distributed port or through the uplink port. See Mark Traffic on a Distributed Port or Uplink Port and Filter Traffic on a Distributed Port or Uplink Port.

Mark Traffic on a Distributed Port or Uplink Port

Assign priority tags in a rule for traffic that needs special treatment such as VoIP and streaming video. You can mark the traffic for a virtual machine, VMkernel adapter, or physical adapter with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

Priority tagging is a mechanism to mark traffic that has higher QoS demands. In this way, the network can recognize different classes of traffic. The network devices can handle the traffic from each class according to its priority and requirements.

You can also re-tag traffic to either raise or lower the importance of the flow. By using a low QoS tag, you can restrict data tagged in a guest operating system.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.

2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. If traffic filtering and marking is not enabled at the port level, click the Enable and reorder button, override the default settings and click **Enable all traffic rules**.

   If traffic rules are enabled at group level, after you override the default settings for the port, the traffic rules are automatically enabled.
5. Click **Add** to create a new rule, or select a rule and click **Edit** to edit it.

   You can change a rule inherited from the distributed port group or uplink port group. In this way, the rule becomes unique within the scope of the port.
6. In the network traffic rule dialog box, select the **Tag** option from the **Action** drop-down menu.
7. Set the priority tag for the traffic within the scope of the rule.

Option	Description
CoS value	Mark the traffic matching the rule with a CoS priority tag in network Layer 2. Select the check box and type a value from 0 to 7.
DSCP value	Mark the traffic associated with the rule with a DSCP tag in network Layer 3. Select the check box and type a value from 0 to 63.

8. Specify the kind of traffic that the rule is applicable to.

   To determine if a data flow is in the scope of a rule for marking or filtering, the vSphere distributed switch examines the direction of the traffic, and properties like source and destination, VLAN, next level protocol, infrastructure traffic type, and so on.

   a) From the **Traffic direction** drop-down menu, select whether the traffic must be ingress, egress, or both so that the rule recognizes it as matching.

      The direction also influences how you are going to identify the traffic source and destination.

   b) By using qualifiers for system data type, Layer 2 packet attributes, and Layer 3 packet attributes set the properties that packets must have to match the rule.

      A qualifier represents a set of matching criteria related to a networking layer. You can match traffic to system data type, Layer 2 traffic properties, and Layer 3 traffic properties. You can use the qualifier for a specific networking layer or can combine qualifiers to match packets more precisely.

      - Use the system traffic qualifier to match packets to the type of virtual infrastructure data that is flowing through the ports of the group . For example, you can select NFS for data transfers to network storage.
      - Use the MAC traffic qualifier to match packets by MAC address, VLAN ID, and next level protocol.

        Locating traffic with a VLAN ID on a distributed port group works with Virtual Guest Tagging (VGT). To match traffic to VLAN ID if Virtual Switch Tagging (VST) is active, use a rule on an uplink port group or uplink port.
      - Use the IP traffic qualifier to match packets by IP version, IP address, and next level protocol and port.
9. In the rule dialog box, click **OK** to save the rule.

Related Links

System Traffic Qualifier on page 2273

By using the system traffic qualifier in a rule for port group or port, you can determine whether certain system data traffic must be marked with a QoS tag, allowed, or dropped.

MAC Traffic Qualifier on page 2274

By using the MAC traffic qualifier in a rule, you can define matching criteria for the Layer 2 (Data Link Layer) properties of packets such as MAC address, VLAN ID, and next level protocol that consumes the frame payload.

IP Traffic Qualifier on page 2275

By using the IP traffic qualifier in a rule, you can define criteria for matching traffic to the Layer 3 (Network Layer) properties such as IP version, IP address, next level protocol, and port.

Filter Traffic on a Distributed Port or Uplink Port

By using a rule, permit or stop traffic for securing data flows through a virtual machine, a VMkernel adapter, or a physical adapter.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.
2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. If traffic filtering and marking is not enabled at the port level, click the Enable and reorder button, override the default settings and click **Enable all traffic rules**.

   If traffic rules are enabled at group level, after you override the default settings for the port, the traffic rules are automatically enabled.
5. Click **Add** to create a new rule, or select a rule and click **Edit** to edit it.

   You can change a rule inherited from the distributed port group or uplink port group. In this way, the rule becomes unique within the scope of the port.
6. In the network traffic rule dialog box, select the **Allow** action to let traffic pass through the distributed port or uplink port, or the **Drop** action to restrict it.
7. Specify the kind of traffic that the rule is applicable to.

   To determine if a data flow is in the scope of a rule for marking or filtering, the vSphere distributed switch examines the direction of the traffic, and properties like source and destination, VLAN, next level protocol, infrastructure traffic type, and so on.

   a) From the **Traffic direction** drop-down menu, select whether the traffic must be ingress, egress, or both so that the rule recognizes it as matching.

      The direction also influences how you are going to identify the traffic source and destination.

   b) By using qualifiers for system data type, Layer 2 packet attributes, and Layer 3 packet attributes set the properties that packets must have to match the rule.

      A qualifier represents a set of matching criteria related to a networking layer. You can match traffic to system data type, Layer 2 traffic properties, and Layer 3 traffic properties. You can use the qualifier for a specific networking layer or can combine qualifiers to match packets more precisely.

      - Use the system traffic qualifier to match packets to the type of virtual infrastructure data that is flowing through the ports of the group . For example, you can select NFS for data transfers to network storage.
      - Use the MAC traffic qualifier to match packets by MAC address, VLAN ID, and next level protocol.
        Locating traffic with a VLAN ID on a distributed port group works with Virtual Guest Tagging (VGT). To match traffic to VLAN ID if Virtual Switch Tagging (VST) is active, use a rule on an uplink port group or uplink port.
      - Use the IP traffic qualifier to match packets by IP version, IP address, and next level protocol and port.

8. In the rule dialog box, click **OK** to save the rule.

Related Links

System Traffic Qualifier on page 2273

By using the system traffic qualifier in a rule for port group or port, you can determine whether certain system data traffic must be marked with a QoS tag, allowed, or dropped.

MAC Traffic Qualifier on page 2274

By using the MAC traffic qualifier in a rule, you can define matching criteria for the Layer 2 (Data Link Layer) properties of packets such as MAC address, VLAN ID, and next level protocol that consumes the frame payload.

IP Traffic Qualifier on page 2275

By using the IP traffic qualifier in a rule, you can define criteria for matching traffic to the Layer 3 (Network Layer) properties such as IP version, IP address, next level protocol, and port.

Working with Network Traffic Rules on a Distributed Port or Uplink Port

Define traffic rules in a distributed port or uplink port group to introduce a policy for processing traffic related to a virtual machine or to a physical adapter. You can filter specific traffic or describe its QoS demands.

View Traffic Rules on a Distributed Port or Uplink Port

Review the traffic rules that form the traffic filtering and marking policy of a distributed port or uplink port.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.
2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. If traffic filtering and marking is not enabled at the port level, click the Enable and reorder button, override the default settings and click **Enable all traffic rules**.

   If traffic rules are enabled at group level, after you override the default settings for the port, the traffic rules are automatically enabled.
5. Examine **Action** to see if the rule filters traffic (Allow or Drop) or marks traffic (Tag) with special QoS demands.
6. From the upper list, select the rule for which you want to view the criteria for locating traffic.

   The traffic qualifying parameters of the rule appear in the Traffic Qualifiers list.

Edit a Traffic Rule on a Distributed Port or Uplink Port

Create or edit traffic rules, and use their parameters to configure a policy for filtering or marking the traffic on a distributed port or uplink port.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.

2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. If traffic filtering and marking is not enabled at the port level, click the Enable and reorder button, override the default settings and click **Enable all traffic rules**.

   If traffic rules are enabled at group level, after you override the default settings for the port, the traffic rules are automatically enabled.
5. Click **Add** to create a new rule, or select a rule and click **Edit** to edit it.

   You can change a rule inherited from the distributed port group or uplink port group. In this way, the rule becomes unique within the scope of the port.

Name the network traffic rule, and deny, allow, or tag the target traffic.

Related Links

Mark Traffic on a Distributed Port or Uplink Port on page 2268

Assign priority tags in a rule for traffic that needs special treatment such as VoIP and streaming video. You can mark the traffic for a virtual machine, VMkernel adapter, or physical adapter with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port or Uplink Port on page 2270

By using a rule, permit or stop traffic for securing data flows through a virtual machine, a VMkernel adapter, or a physical adapter.

Change Rule Priorities on a Distributed Port or Uplink Port

Reorder the rules that form the traffic filtering and marking policy of a distributed port or uplink port to change the sequence of actions for analyzing traffic for security and QoS.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

The vSphere distributed switch applies network traffic rules in a strict order. If a packet already satisfies a rule, the packet might not be passed to the next rule in the policy.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.
2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. Click the **Enable and reorder** button.
5. If traffic filtering and marking is not enabled at the port level, override the default settings and click Enable all traffic rules.

   If traffic rules are enabled at group level, after you override the default settings for the port, the traffic rules are automatically enabled.
6. Select a rule and use the **Move up** or **Move down** button to change its priority.
7. Click **OK** to apply the changes.

Delete a Traffic Rule on a Distributed Port or Uplink Port

Delete a traffic rule on a distributed port or uplink port to stop filtering or marking certain type of packets that are flowing to a virtual machine or a physical adapter.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.
2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. If traffic filtering and marking is not enabled at the port level, click the Enable and reorder button, override the default settings and click **Enable all traffic rules**.

   If traffic rules are enabled at group level, after you override the default settings for the port, the traffic rules are automatically enabled.
5. Select the rule and click the **Delete** button.
6. Click **OK**.

Disable Traffic Filtering and Marking on a Distributed Port or Uplink Port

Disable the traffic filtering and marking policy on a port to let traffic flow to a virtual machine or a physical adapter without filtering for security or marking for QoS.

To override a policy on distributed port level, enable the port-level override option for this policy. See Configure Overriding Networking Policies on Port Level.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.
2. Select a port from the list.
3. Select the **Traffic Filtering and Marking** tab.
4. Click the **Enable and reorder** button.
5. Use the toggle buttons to override the default settings at the port level and disable all traffic rules.
6. Click **OK**.

Qualifying Traffic for Filtering and Marking

The traffic that you want to filter or want to mark with QoS tags can be matched to the type of carried infrastructure data, such as data for storage, vCenter Server management, and so on, and to Layer 2 and Layer 3 properties.

To match the traffic in the scope of the rule more precisely, you can combine criteria for system data type, Layer 2 header, and Layer 3 header.

System Traffic Qualifier

By using the system traffic qualifier in a rule for port group or port, you can determine whether certain system data traffic must be marked with a QoS tag, allowed, or dropped.

System Traffic Type

You can select the type of traffic through the ports of the group that carries system data, that is, traffic for management from vCenter Server, storage, VMware vSphere®vMotion®, and vSphere Fault Tolerance. You can mark or filter only a specific traffic type, or for all system data traffic except for a infrastructure feature. For example, you can mark with a QoS value or filter the traffic for management from vCenter Server , storage and vMotion, but not the traffic carrying the Fault Tolerance data.

Related Links

Mark Traffic on a Distributed Port Group or Uplink Port Group on page 2263
Assign priority tags to traffic, such as VoIP and streaming video, that has higher networking requirements for bandwidth, low latency, and so on. You can mark the traffic with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port Group or Uplink Port Group on page 2265
Allow or stop traffic for securing the data that flows through the ports of a distributed port group or uplink port group.

Mark Traffic on a Distributed Port or Uplink Port on page 2268
Assign priority tags in a rule for traffic that needs special treatment such as VoIP and streaming video. You can mark the traffic for a virtual machine, VMkernel adapter, or physical adapter with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port or Uplink Port on page 2270
By using a rule, permit or stop traffic for securing data flows through a virtual machine, a VMkernel adapter, or a physical adapter.

MAC Traffic Qualifier

By using the MAC traffic qualifier in a rule, you can define matching criteria for the Layer 2 (Data Link Layer) properties of packets such as MAC address, VLAN ID, and next level protocol that consumes the frame payload.

Protocol Type

The **Protocol type** attribute of the MAC traffic qualifier corresponds to the EtherType field in Ethernet frames. EtherType represents the type of next level protocol that is going to consume the payload of the frame.

You can select a protocol from the drop-down menu or type its hexadecimal number. For example, to capture traffic for the Link Layer Discovery Protocol (LLDP) protocol, type `88CC`.

VLAN ID

You can use the VLAN ID attribute of the MAC traffic qualifier to mark or filter traffic in a particular VLAN.

Note:

The VLAN ID qualifier on a distributed port group works with Virtual Guest Tagging (VGT).

If a flow is tagged with a VLAN ID through Virtual Switch Tagging (VST), it cannot be located by using this ID in a rule on a distributed port group or distributed port. The reason is that the distributed switch checks the rule conditions, including the VLAN ID, after the switch has already untagged the traffic. In this case, to match traffic by VLAN ID successfully, you must use a rule on an uplink port group or uplink port.

Source Address

By using the Source Address group of attributes, you can match packets by the source MAC address or network.

You can use a comparison operator to mark or filter packets that have or do not have the specified source address or network.

You can match the traffic source in several ways.

Table 186: Patterns for Filtering or Marking Traffic by MAC Source Address

Parameters to Match Traffic Source Address	Comparison Operator	Networking Argument Format
MAC address	**is** or **is not**	Type the MAC address for matching. Use colons to separate the octets in it.
MAC network	**matches** or **does not match**	Type the lowest address in the network and a mask. Set ones at the positions of the network bits, and zeroes for the host part.

For example, for a MAC network with prefix 05:50:56 that is 23 bits long, set the address as `00:50:56:00:00:00` and mask as `ff:ff:fe:00:00:00`.

Destination Address

By using the Destination Address group of attributes, you can match packets to their destination address. The MAC destination address options have the same format as those for the source address.

Comparison Operators

To match traffic in a MAC qualifier more closely to your needs, you can use affirmative comparison or negation. You can use operators such that all packets except the ones with certain attributes fall in the scope of a rule.

Related Links

Mark Traffic on a Distributed Port Group or Uplink Port Group on page 2263
Assign priority tags to traffic, such as VoIP and streaming video, that has higher networking requirements for bandwidth, low latency, and so on. You can mark the traffic with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port Group or Uplink Port Group on page 2265
Allow or stop traffic for securing the data that flows through the ports of a distributed port group or uplink port group.

Mark Traffic on a Distributed Port or Uplink Port on page 2268
Assign priority tags in a rule for traffic that needs special treatment such as VoIP and streaming video. You can mark the traffic for a virtual machine, VMkernel adapter, or physical adapter with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port or Uplink Port on page 2270
By using a rule, permit or stop traffic for securing data flows through a virtual machine, a VMkernel adapter, or a physical adapter.

IP Traffic Qualifier

By using the IP traffic qualifier in a rule, you can define criteria for matching traffic to the Layer 3 (Network Layer) properties such as IP version, IP address, next level protocol, and port.

Protocol

The **Protocol** attribute of the IP traffic qualifier represents the next level protocol consuming the payload of the packet. You can select a protocol from the drop-down menu or type its decimal number according to RFC 1700.

For the TCP and UDP protocols, you can also match traffic by source and destination ports.

Source Port

By using the Source port attribute, you can match TCP or UDP packets by the source port. Consider the traffic direction when matching traffic to a source port.

Destination Port

By using the Destination port attribute, you can match TCP or UDP packets by the destination port. Consider the traffic direction when matching traffic to a destination port.

Source Address

By using the Source Address attribute, you can match packets by source address or subnet. Consider the traffic direction when matching traffic to a source address or network.

You can match traffic source in several ways.

Table 187: Patterns for Filtering or Marking Traffic by IP Source Address

Parameters to Match Traffic Source Address	Comparison Operator	Networking Argument Format
IP version	**any**	Select the IP version from the drop-down menu.
IP address	**is** or **is not**	Type the IP address that you want to match.
IP subnet	**matches** or **does not match**	Type the lowest address in the subnet and the bit length of the subnet prefix.

Destination Address

Use the Destination Address to match packets by IP address, subnet, or IP version. The destination address has the same format as the one for the source.

Comparison Operators

To match traffic in an IP qualifier more closely to your needs, you can use affirmative comparison or negation. You can define that all packets fall in the scope of a rule except packets with certain attributes.

Related Links

Mark Traffic on a Distributed Port Group or Uplink Port Group on page 2263

Assign priority tags to traffic, such as VoIP and streaming video, that has higher networking requirements for bandwidth, low latency, and so on. You can mark the traffic with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port Group or Uplink Port Group on page 2265

Allow or stop traffic for securing the data that flows through the ports of a distributed port group or uplink port group.

Mark Traffic on a Distributed Port or Uplink Port on page 2268
Assign priority tags in a rule for traffic that needs special treatment such as VoIP and streaming video. You can mark the traffic for a virtual machine, VMkernel adapter, or physical adapter with a CoS tag in Layer 2 of the network protocol stack or with a DSCP tag in Layer 3.

Filter Traffic on a Distributed Port or Uplink Port on page 2270
By using a rule, permit or stop traffic for securing data flows through a virtual machine, a VMkernel adapter, or a physical adapter.

Manage Policies for Multiple Port Groups on a vSphere Distributed Switch

You can modify networking policies for multiple port groups on a vSphere Distributed Switch.

Create a vSphere Distributed Switch with one or more port groups.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch in the object navigator and select **Distributed Port Group** > **Manage Distributed Port Groups**.
3. On the Select port group policies page, select the check box next to the policy categories to modify and click **Next**.

Option	Description
Security	Set MAC address changes, forged transmits, and promiscuous mode for the selected port groups.
Traffic shaping	Set the average bandwidth, peak bandwidth, and burst size for inbound and outbound traffic on the selected port groups.
VLAN	Configure how the selected port groups connect to physical VLANs.
Teaming and failover	Set load balancing, failover detection, switch notification, and failover order for the selected port groups.
Resource allocation	Set network resource pool association for the selected port groups.
Monitoring	Enable or disable NetFlow on the selected port groups.
Miscellaneous	Enable or disable port blocking on the selected port groups.

4. On the Select port groups page, select the distributed port group(s) to edit and click **Next**.
5. Optional: On the Security page, use the drop-down menus to edit the security exceptions and click **Next**.

Option	Description
Promiscuous mode	• **Reject**. Placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter. • **Accept**. Placing a guest adapter in promiscuous mode causes it to detect all frames passed on the vSphere Distributed Switch that are allowed under the VLAN policy for the port group that the adapter is connected to.
MAC address changes	• **Reject**. If set to **Reject** and the guest operating system changes the MAC address of the adapter to anything other than what is in the `.vmx` configuration file, all inbound frames are dropped. If the Guest OS changes the MAC address back to match the MAC address in the `.vmx` configuration file, inbound frames are passed again. • **Accept**. Changing the MAC address from the Guest OS has the intended effect. Frames to the new MAC address are received.

Option	Description
Forged transmits	• **Reject**. Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped. • **Accept**. No filtering is performed and all outbound frames are passed.

6. Optional: On the VLAN page, use the drop-down menus to edit the VLAN policy and click **Next**.

Option	Description
None	Do not use VLAN.
VLAN	In the **VLAN ID** field, enter a number between 1 and 4094.
VLAN trunking	Enter a **VLAN trunk range**.
Private VLAN	Select an available private VLAN to use.

7. Optional: On the Traffic shaping page, use the drop-down menus to enable or disable Ingress or Egress traffic shaping and click **Next**.

Option	Description
Status	If you enable either **Ingress traffic shaping** or **Egress traffic shaping**, you are setting limits on the amount of networking bandwidth allocated for each VMkernel adapter or virtual network adapter associated with this port group. If you disable the policy, services have a free, clear connection to the physical network by default.
Average bandwidth	Establishes the number of bits per second to allow across a port, averaged over time, that is, the allowed average load.
Peak bandwidth	The maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This maximum number tops the bandwidth used by a port whenever it is using its burst bonus.
Burst size	The maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by **Average bandwidth**, it might be allowed to transmit data at a higher speed if a burst bonus is available. This parameter tops the number of bytes that can be accumulated in the burst bonus and transferred at a higher speed.

8. Optional: On the Teaming and failover page, use the drop-down menus to edit the settings and click **Next**.

Option	Description
Load balancing	IP-based teaming requires that the physical switch be configured with ether channel. For all other options, ether channel should be disabled. Select how to choose an uplink. • **Route based on the originating virtual port**. Choose an uplink based on the virtual port where the traffic entered the distributed switch. • **Route based on IP hash**. Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash. • **Route based on source MAC hash**. Choose an uplink based on a hash of the source Ethernet.

Option	Description
	• **Route based on physical NIC load**. Choose an uplink based on the current loads of physical NICs. • **Use explicit failover order**. Always use the highest order uplink, from the list of Active adapters, which passes failover detection criteria.
Network failure detection	Select the method to use for failover detection. • **Link status only**. Relies solely on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch. • **Beacon probing**. Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. Do not use beacon probing with IP-hash load balancing.
Notify switches	Select **Yes** or **No** to notify switches in the case of failover. Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. If you select **Yes**, whenever a virtual NIC is connected to the distributed switch or whenever that virtual NIC's traffic is routed over a different physical NIC in the team because of a failover event, a notification is sent out over the network to update the lookup tables on physical switches. Use this process for the lowest latency of failover occurrences and migrations with vMotion. If the **Notify switches** is set to **Yes**, then all the connected ports, port groups, and distributed switches are connected back to the host when vCenter Server reconnects with ESXi hosts.
Failback	Select **Yes** or **No** to disable or enable failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. • **Yes** (default). The adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. • **No**. A failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
Failover order	Select how to distribute the work load for uplinks. To use some uplinks but reserve others in case the uplinks in use fail, set this condition by moving them into different groups. • **Active uplinks**. Continue to use the uplink when the network adapter connectivity is up and active. • **Standby uplinks** . Use this uplink if one of the active adapter's connectivity is down. When using IP-hash load balancing, do not configure standby uplinks. • **Unused uplinks** . Do not use this uplink.

9. Optional: On the Resource allocation page, use the **Network resource pool** drop-down menu to add or remove resource allocations and click **Next**.
10. Optional: On the Monitoring page, use the drop-down menu to enable or disable NetFlow and click **Next**.

Option	Description
Disabled	NetFlow is disabled on the distributed port group.
Enabled	NetFlow is enabled on the distributed port group. You can configure NetFlow settings at the vSphere Distributed Switch level.

11. Optional: On the Miscellaneous page, select **Yes** or **No** from the drop-down menu and click **Next**.

    Select**Yes** to shut down all ports in the port group. This shutdown might disrupt the normal network operations of the hosts or virtual machines using the ports.
12. Review your settings on the Ready to complete page and click **Finish**.

    Use the **Back** button to change any settings.

Port Blocking Policies

Port blocking policies allow you to selectively block ports from sending or receiving data.

Edit the Port Blocking Policy for a Distributed Port Group

You can block all ports in a distributed port group.

Blocking the ports of a distributed port group might disrupt the normal network operations of the hosts or virtual machines using the ports.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Right-click the distributed switch in the object navigator and select **Distributed Port Group** > **Manage Distributed Port Groups**.
3. Select the **Miscellaneous** check box and click **Next**.
4. Select one or more distributed port group to configure and click **Next**.
5. From the **Block all ports** drop-down menu, enable or disable port blocking, and click **Next**.
6. Review your settings and click **Finish**.

Edit the Blocking Policy for a Distributed Port or Uplink Port

You can block an individual distributed port or uplink port.

Enable the port-level overrides. See Configure Overriding Networking Policies on Port Level

Blocking the flow through a port might disrupt the normal network operations on the host or virtual machine using the port.

1. Navigate to a distributed switch and then navigate to a distributed port or an uplink port.
   - To navigate to the distributed ports of the switch, click **Networks** > **Distributed Port Groups**, click a distributed port group from the list, and click the **Ports** tab.
   - To navigate to the uplink ports of an uplink port group, click **Networks** > **Uplink Port Groups**, click an uplink port group from the list, and click the **Ports** tab.

2. Select a port from the list.
3. Click **Edit distributed port settings**.
4. In the **Miscellaneous** section, select the **Override** check box, and from the drop-down menu enable or disable port blocking.
5. Click **OK**.

MAC Learning Policy

MAC learning provides network connectivity to deployments where multiple MAC addresses are used from one vNIC.

For example, in a nested hypervisor deployment where an ESXi VM runs on an ESXi host and multiple VMs run inside the ESXi VM. Without MAC learning, when the ESXi VM's vNIC connects to a switch port, it only contains a static MAC address. VMs running inside the ESXi VM do not have network connectivity because their packets have different source MAC addresses. With MAC learning, the vSwitch inspects the source MAC address of every packet coming from the vNIC, learns the MAC address in its MAC table, and allows the packet to pass. If a MAC address that is learned is not used for a certain period of time, it is removed.

MAC learning also supports unknown unicast flooding. Normally, when a packet that is received by a port has an unknown destination MAC address, the packet is dropped. With unknown unicast flooding enabled, the port floods unknown unicast traffic to every port on the switch that has MAC learning and unknown unicast flooding enabled. This property is enabled by default, but only if MAC learning is enabled.

The number of MAC addresses that can be learned is configurable. The maximum value is 4096 per port, which is the default. You can also set the policy for when the limit is reached. The options are:

- Drop - Packets from an unknown source MAC address are dropped. Packets inbound to this MAC address will be treated as unknown unicast. The port will receive the packets only if it has unknown unicast flooding enabled.
- Allow - Packets from an unknown source MAC address are forwarded although the address will not be learned. Packets inbound to this MAC address will be treated as unknown unicast. The port will receive the packets only if it has unknown unicast flooding enabled.

In vSphere 6.7 and later, MAC Learning can be enabled on a Distributed Virtual Port group using the vSphere API. You can configure the MAC Learning Policy on vSphere Distributed Switch, Distributed Virtual Port Group, and Distributed Virtual Port. If a MAC learning policy is not set on Distributed Virtual Port Group, it is inherited from vSphere Distributed Switch and if it is not enabled on the DVport, it is inherited from Distributed Virtual Port Group. See *vSphere Web Services API Reference* for more information.

Isolating Network Traffic by Using VLANs

VLANs let you segment a network into multiple logical broadcast domains at Layer 2 of the network protocol stack.

VLAN Configuration

Virtual LANs (VLANs) enable a single physical LAN segment to be further isolated so that groups of ports are isolated from one another as if they were on physically different segments.

Benefits of Using VLANs in vSphere

The VLAN configuration in a vSphere environment provides certain benefits.

- Integrates ESXi hosts into a pre-existing VLAN topology.
- Isolates and secures network traffic.
- Reduces congestion of network traffic.

Watch the video about the benefits and main principles in introducing VLANs in a vSphere environment.

VLAN Tagging Modes

vSphere supports three modes of VLAN tagging in ESXi: External Switch Tagging (EST), Virtual Switch Tagging (VST), and Virtual Guest Tagging (VGT).

Tagging Mode	VLAN ID on switch port groups	Description
EST	0	The physical switch performs the VLAN tagging. The host network adapters are connected to access ports on the physical switch.
VST	Between 1 and 4094	The virtual switch performs the VLAN tagging before the packets leave the host. The host network adapters must be connected to trunk ports on the physical switch.
VGT	• 4095 for standard switch • Range of and individual VLANs for distributed switch	The virtual machine performs the VLAN tagging. The virtual switch preserves the VLAN tags when it forwards the packets between the virtual machine networking stack and external switch. The host network adapters must be connected to trunk ports on the physical switch. The vSphere Distributed Switch supports a modification of VGT. For security reasons, you can configure a distributed switch to pass only packets that belong to particular VLANs. **Note:** For VGT you must have an 802.1Q VLAN trunking driver installed on the guest operating system of the virtual machine.

Watch the video that explains the modes of VLAN tagging in virtual switches.

Related Links

Edit a Standard Switch Port Group on page 2152

By using the vSphere Client, you can edit the name and VLAN ID of a standard switch port group, and override networking policies at the port group level.

Add a Virtual Machine Port Group on page 2151

Add VM port groups on a vSphere Standard Switch to provide connectivity and common network configuration for virtual machines.

Configure VLAN Tagging on a Distributed Port Group or Distributed Port on page 2254

To apply VLAN tagging globally on all distributed ports, you must set the VLAN policy on a distributed port group. To integrate the virtual traffic on the port with physical VLANs in a different way from the parent distributed port group, you must use the VLAN policy on a distributed port.

Private VLANs

Private VLANs are used to solve VLAN ID limitations by adding a further segmentation of the logical broadcast domain into multiple smaller broadcast subdomains.

A private VLAN is identified by its primary VLAN ID. A primary VLAN ID can have multiple secondary VLAN IDs associated with it. Primary VLANs are **Promiscuous**, so that ports on a private VLAN can communicate with ports

configured as the primary VLAN. Ports on a secondary VLAN can be either **Isolated**, communicating only with promiscuous ports, or **Community**, communicating with both promiscuous ports and other ports on the same secondary VLAN.

To use private VLANs between a host and the rest of the physical network, the physical switch connected to the host needs to be private VLAN-capable and configured with the VLAN IDs being used by ESXi for the private VLAN functionality. For physical switches using dynamic MAC+VLAN ID based learning, all corresponding private VLAN IDs must be first entered into the switch's VLAN database.

Create a Private VLAN

Create the necessary private VLANs on the vSphere Distributed Switch to be able to assign distributed ports to participate to a private VLAN.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **Private VLAN** .
3. Click **Edit**.
4. To add a primary VLAN, above Primary VLAN ID click the **plus sign (+)** button.
   The primary private VLAN also appears under Secondary Private VLAN ID.
5. To add a secondary VLAN, in the right pane click the **plus sign (+)**button.
6. From the drop-down menu in the **Secondary VLAN type** column, select either **Isolated** or **Community**.
7. Click **OK**.

Configure a distributed port group or port to associate traffic with the private VLAN. See Configure VLAN Tagging on a Distributed Port Group or Distributed Port.

Related Links

Configure VLAN Tagging on a Distributed Port Group or Distributed Port on page 2254

To apply VLAN tagging globally on all distributed ports, you must set the VLAN policy on a distributed port group. To integrate the virtual traffic on the port with physical VLANs in a different way from the parent distributed port group, you must use the VLAN policy on a distributed port.

Remove a Primary Private VLAN

Remove unused primary VLANs from the configuration of a vSphere Distributed Switch.

Verify that no port groups are configured to use the primary VLAN and its associated secondary VLANs.

When you remove a primary private VLAN, you also remove the associated secondary private VLANs.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **Private VLAN**.
3. Click **Edit**.
4. Select the primary private VLAN to remove.
5. Click the **times sign (x)** button abovethe Primary VLAN ID list.
6. Click **OK.**

Remove a Secondary Private VLAN

Remove unused secondary private VLANs from the configuration of a vSphere Distributed Switch.

Verify that no port groups are configured to use the secondary VLAN.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **Private VLAN**.
3. Click **Edit**.
4. Select a primary private VLAN.
   The secondary private VLANs associated with it appear on the right.
5. Select the secondary private VLAN to remove.
6. Above the secondary VLAN ID list, click the **times sign (x)**button and click **OK**.

Managing Network Resources

vSphere provides several different methods to help you manage your network resources.

DirectPath I/O

DirectPath I/O allows virtual machine access to physical PCI functions on platforms with an I/O Memory Management Unit.

The following features are unavailable for virtual machines configured with DirectPath:

- Hot adding and removing of virtual devices
- Suspend and resume
- Record and replay
- Fault tolerance
- High availability
- DRS (limited availability. The virtual machine can be part of a cluster, but cannot migrate across hosts)
- Snapshots

Enable Passthrough for a Network Device on a Host

Passthrough devices provide the means to use resources efficiently and improve performance of your environment. You can enable DirectPath I/O passthrough for a network device on a host.

CAUTION: If your ESXi host is configured to boot from a USB device or an SD card attached to a USB channel, make sure that you do not enable DirectPath I/O passthrough for the USB controller. Passing through a USB controller on an ESXi host that boots from a USB device or SD card might put the host in a state where its configuration cannot be persisted.

1. Browse to a host in the vSphere Client navigator.
2. On the **Configure** tab, expand **Hardware** and click **PCI Devices**.
3. To enable DirectPath I/O passthrough for a PCI network device on the host, click **Edit**.
   A list of available passthrough devices appears.

Icon	Description
green icon	A device is active and can be enabled.
orange icon	The state of the device has changed, and you must reboot the host before you can use the device.

4. Select the network device to be used for passthrough and click **OK**.
   The selected PCI device appears in the table. Device information is displayed at the bottom of the screen.

Configure a PCI Device on a Virtual Machine

Passthrough devices provide the means to more efficiently use resources and improve performance in your environment. You can configure a passthrough PCI device on a virtual machine in the vSphere Client.

Verify that a passthrough networking device is configured on the host of the virtual machine. See Enable Passthrough for a Network Device on a Host.

When using passthrough devices with a Linux kernel version 2.6.20 or earlier, avoid MSI and MSI-X modes because these modes have significant performance impact.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. Power off the virtual machine.
3. From the Actions menu, select Edit Settings.
4. Select the **Virtual Hardware** tab in the dialog box displaying the settings.
5. Expand the **Memory** section, and set the **Limit** to **Unlimited**.
6. Click the **Add new device** button and under Other devices, select **PCI Device**.
   The **New PCI device** drop-down menu is added to the list in the **Virtual Hardware** tab.
7. From the **New PCI device** drop-down menu select the passthrough device to use, and click **OK**.
8. Power on the virtual machine.

Adding a DirectPath I/O device to a virtual machine sets memory reservation to the memory size of the virtual machine.

Single Root I/O Virtualization (SR-IOV)

vSphere supports Single Root I/O Virtualization (SR-IOV). You can use SR-IOV for networking of virtual machines that are latency sensitive or require more CPU resources.

Overview of SR-IOV

SR-IOV is a specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear as multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices. PFs are full PCIe functions that are capable of configuring and managing the SR-IOV functionality. It is possible to configure or control PCIe devices using PFs, and the PF has full ability to move data in and out of the device. VFs are lightweight PCIe functions that support data flowing but have a restricted set of configuration resources.

The number of virtual functions provided to the hypervisor or the guest operating system depends on the device. SR-IOV enabled PCIe devices require appropriate BIOS and hardware support, as well as SR-IOV support in the guest operating system driver or hypervisor instance. See SR-IOV Support.

Using SR-IOV in vSphere

In vSphere, a virtual machine can use an SR-IOV virtual function for networking. The virtual machine and the physical adapter exchange data directly without using the VMkernel as an intermediary. Bypassing the VMkernel for networking reduces latency and improves CPU efficiency.

In vSphere, though a virtual switch (standard switch or distributed switch) does not handle the network traffic of an SR-IOV enabled virtual machine connected to the switch, you can control the assigned virtual functions by using switch configuration policies at port group or port level.

SR-IOV Support

vSphere supports SR-IOV in an environment with specific configuration only. Some features of vSphere are not functional when SR-IOV is enabled.

Supported Configurations

To use SR-IOV in vSphere, your environment must meet several configuration requirements.

Table 188: Supported Configurations for Using SR-IOV

Component	Requirements
Physical host	• Must be compatible with the release. • Must have an Intel or AMD processor. • Must support I/O memory management unit (IOMMU), and must have IOMMU enabled in the BIOS. • Must support SR-IOV, and must have SR-IOV enabled in the BIOS. Contact the server vendor to determine whether the host supports SR-IOV.
Physical NIC	• Must be compatible with the release. • Must be supported for use with the host and SR-IOV according to the technical documentation from the server vendor. • Must have SR-IOV enabled in the firmware. • Must use MSI-X interrupts.
PF driver in ESXi for the physical NIC	• Must be certified by VMware. • Must be installed on the host. The release provides a default driver for certain NICs, while for others you must download and manually install it.
Guest OS	Must be supported by the NIC on the installed release according to the technical documentation from the NIC vendor.
VF driver in the guest OS	• Must be compatible with the NIC. • Must be supported on the guest OS release according to the technical documentation from the NIC vendor. • Must be Microsoft WLK or WHCK certified for Windows virtual machines. • Must be installed on the operating system. The operating system release contains a default driver for certain NICs, while for others you must download and install it from a location provided by the vendor of the NIC or the host.

To verify that your physical hosts and NICs are compatible with releases, see the *VMware Compatibility Guide*.

Availability of Features

The following features are not available for virtual machines configured with SR-IOV:

- vSphere vMotion

- Storage vMotion
- vShield
- NetFlow
- VXLAN Virtual Wire
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- Virtual machine suspend and resume
- Virtual machine snapshots
- MAC-based VLAN for passthrough virtual functions
- Hot addition and removal of virtual devices, memory, and vCPU
- Participation in a cluster environment
- Network statistics for a virtual machine NIC using SR-IOV passthrough

Note: Attempts to enable or configure unsupported features with SR-IOV in the result in unexpected behavior in your environment.

Supported NICs

All NICs must have drivers and firmware that support SR-IOV. Some NICs might require SR-IOV to be enabled on the firmware. To learn what NICs are supported for virtual machines configured with SR-IOV, see the VMware Compatibility Guide.

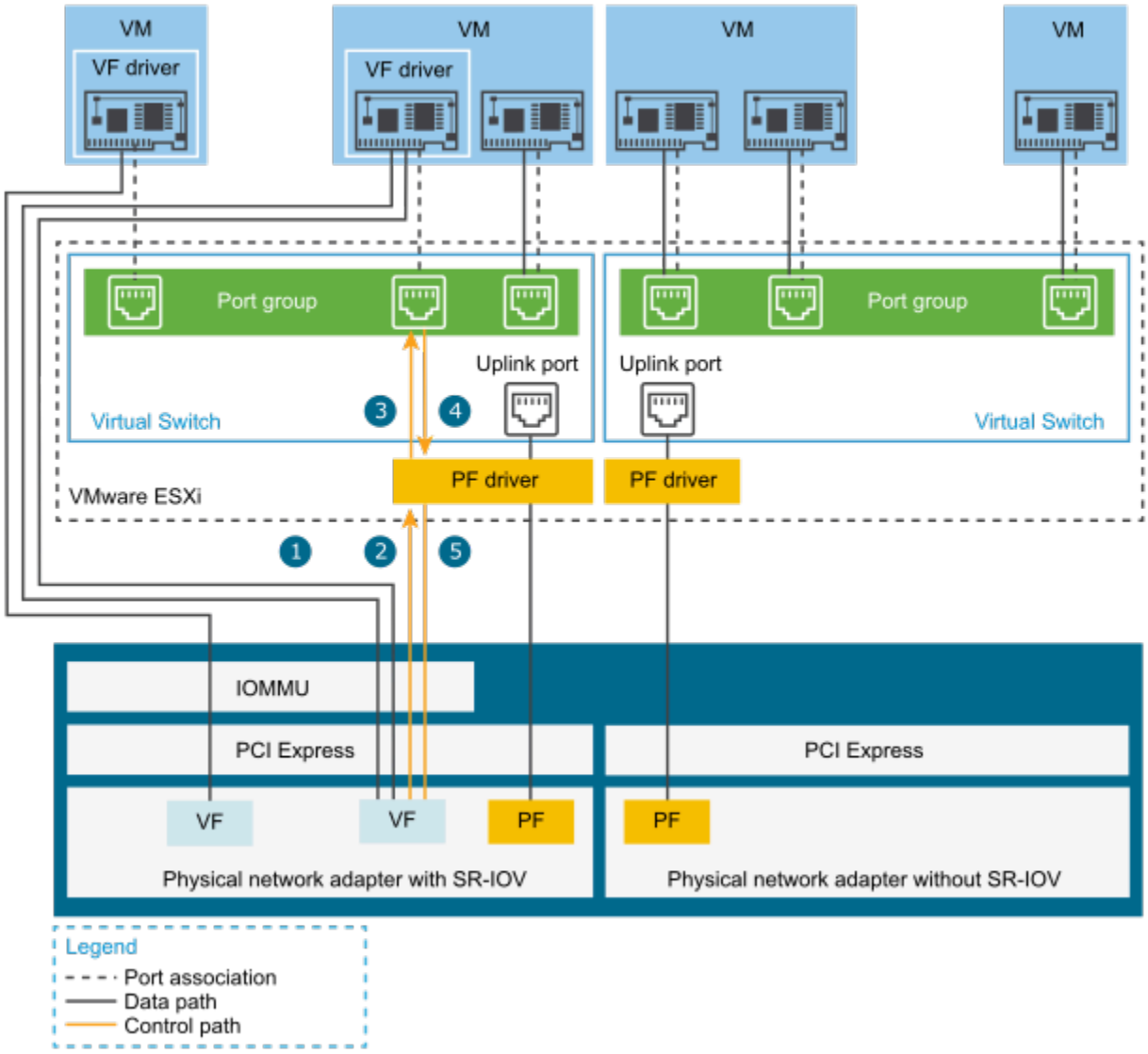
SR-IOV Component Architecture and Interaction

vSphere SR-IOV support relies on the interaction between the virtual functions (VFs) and the physical function (PF) of the NIC port for better performance, and interaction between the driver of the PF and the host switch for traffic control.

In a host that runs virtual machine traffic on top of SR-IOV physical adapters, virtual machine adapters directly contact the virtual functions to communicate data. However, the ability to configure networks is based on the active policies for the port holding the virtual machines.

On an ESXi host without SR-IOV, the virtual switch sends external network traffic through its ports on the host from or to the physical adapter for the relevant port group. The virtual switch also applies the networking policies on managed packets.

Figure 57: Data and Configuration Paths in the SR-IOV Support of vSphere



The data path directly connects the virtual machine with the virtual function on the NIC. The control path includes the virtual switch and the active policies on the virtual machine.

Data Path in SR-IOV

After the virtual machine network adapter is assigned to a virtual function, the VF driver in the guest operating system uses the I/O memory management unit (IOMMU) technology to access the virtual function that must receive or send the data over the network. The VMkernel, that is, the virtual switch in particular, does not process the data flow, which reduces the overall latency of SR-IOV enabled workloads.

Configuration Path in SR-IOV

If the guest operating system attempts to change the configuration of a virtual machine adapter mapped to a VF, the change takes place if it is allowed by the policy on the port associated with the virtual machine adapter.

The configuration workflow consists of the following operations:

1. The guest operating system requests a configuration change on the VF.
2. The VF forwards the request to the PF through a mailbox mechanism.
3. The PF driver checks the configuration request with the virtual switch (standard switch or host proxy switch of a distributed switch).
4. The virtual switch verifies the configuration request against the policy on the port with which the VF enabled virtual machine adapter is associated.
5. The PF driver configures the VF if the new settings are in compliance with the port policy of the virtual machine adapter.

   For example, if the VF driver tries to modify the MAC address, the address remains the same if MAC address change is not allowed in the security policy for the port group or port. The guest operating system might show that the change is successful but a log message indicates that the operation has failed. As a result, the guest operating system and the virtual device save different MAC addresses. The network interface in the guest operating system might not be able to acquire an IP address and communicate. In this case, you have to reset the interface in the guest operating system to get the latest MAC address from the virtual device and acquire an IP address.

vSphere and Virtual Function Interaction

Virtual functions (VFs) are lightweight PCIe functions that contain all the resources necessary for data exchange but have a minimized set of configuration resources. Interaction between vSphere and VFs is limited.

- The physical NIC must use MSI-X interrupts.
- VFs do not implement rate control in vSphere. Every VF can potentially use the entire bandwidth of a physical link.
- When a VF device is configured as a passthrough device on a virtual machine, the standby and hibernate functions for the virtual machine are not supported.
- The maximum number of VFs that you can create and the maximum number of VFs that you can use for passthrough are different. The maximum number of VFs that you can instantiate depends on the NIC capability and on the hardware configuration of the host. However, due to the limited number of interrupt vectors available for passthrough devices, only a limited number of all instantiated VFs can be used on an ESXi host.

  The total number of interrupt vectors on each ESXi host can scale up to 4096 in the case of 32 CPUs. When the host boots, devices on the host such as storage controllers, physical network adapters, and USB controllers consume a subset of the 4096 vectors. If these devices require more than 1024 vectors, the maximum number of potentially supported VFs is reduced.
- The number of VFs that is supported on an Intel NIC can be different from the number that is supported on an Emulex NIC. See the technical documentation from the NIC vendor.
- If you have Intel and Emulex NICs present with SR-IOV enabled, the number of VFs available for the Intel NICs depends on how many VFs are configured for the Emulex NIC, and the reverse. You can use the following formula to estimate the maximum number of VFs for use if all 3072 interrupt vectors are available for passthrough:

  ```
  3X + 2Y < 3072
  ```

  where `X` is the number of Intel VFs, and `Y` is the number of Emulex VFs.

  This number can be smaller if other types of devices on the host use more than 1024 interrupt vectors from the total of 4096 vectors on the host.
- vSphere SR-IOV supports up to 1024 VFs on a supported Intel and Emulex NICs.
- vSphere SR-IOV supports up to 64 VFs on a supported Intel or Emulex NIC.
- If a supported Intel NIC loses connection, all VFs from the physical NIC stop communication, including that between VFs.
- If a supported Emulex NIC loses connection, all VFs stop communication with the external environment, but communication between VFs still works.
- VF drivers offer many different features, such as IPv6 support, TSO, and LRO checksum. See the technical documentation of the NIC vendor for more details.

Related Links

Virtual Machine That Uses an SR-IOV Virtual Function Fails to Power On Because the Host Is Out of Interrupt Vectors on page 2294

On an ESXi host, one or more virtual machines that use SR-IOV virtual functions (VFs) for networking are powered off.

DirectPath I/O vs SR-IOV

SR-IOV offers performance benefits and tradeoffs similar to those of DirectPath I/O. DirectPath I/O and SR-IOV have similar functionality but you use them to accomplish different things.

SR-IOV is beneficial in workloads with very high packet rates or very low latency requirements. Like DirectPath I/O, SR-IOV is not compatible with certain core virtualization features, such as vMotion. SR-IOV does, however, allow for a single physical device to be shared amongst multiple guests.

With DirectPath I/O you can map only one physical function to one virtual machine. SR-IOV lets you share a single physical device, allowing multiple virtual machines to connect directly to the physical function.

Configure a Virtual Machine to Use SR-IOV

To use the capabilities of SR-IOV, you must enable the SR-IOV virtual functions on the host and connect a virtual machine to the functions.

Verify that the configuration of your environment supports SR-IOV. See SR-IOV Support.

The traffic passes from an SR-IOV passthrough adapter to the physical adapter in compliance with the active policy on the associated port on the standard or distributed switch.

To examine which virtual function is assigned to an SR-IOV passthrough network adapter, on the **Summary** tab for the virtual machine expand the **VM Hardware** panel and check the properties of the adapter.

The topology diagram of the switch marks virtual machine adapters that use virtual functions with the icon.

Set up the traffic passing through the virtual functions attached to the virtual machine by using the networking policies on the switch, port group, and port. See Networking Options for the Traffic Related to an SR-IOV Enabled Virtual Machine.

Enable SR-IOV on a Host Physical Adapter

Before you can connect virtual machines to virtual functions, use the vSphere Client to enable SR-IOV and set the number of virtual functions on your host.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Physical adapters**.
   You can look at the SR-IOV property to see whether a physical adapter supports SR-IOV.
3. Select the physical adapter and click **Edit adapter settings**.
4. Under SR-IOV, select **Enabled** from the **Status** drop-down menu.
5. In the **Number of virtual functions** text box, type the number of virtual functions that you want to configure for the adapter.
   A value of 0 means SR-IOV is not enabled for that physical function.
6. Click **OK**.
7. Restart the host.

The virtual functions become active on the NIC port represented by the physical adapter entry. They appear in the PCI Devices list in the **Settings** tab for the host.

You can use the `esxcli network sriovnic` vCLI commands to examine the configuration of virtual functions on the host.

Associate a virtual machine with a virtual function through an SR-IOV passthrough network adapter.

Assign a Virtual Function as SR-IOV Passthrough Adapter to a Virtual Machine

To ensure that a virtual machine and a physical NIC can exchange data, you must associate the virtual machine with one or more virtual functions as SR-IOV passthrough network adapters.

- Verify that the virtual functions exist on the host.
- Verify that the passthrough networking devices for the virtual functions are active in the PCI Devices list on the **Settings** tab for the host.
- Verify that the virtual machine compatibility is ESXi 5.5 and later.
- Verify that Red Hat Enterprise Linux 6 and later or Windows has been selected as the guest operating system when the virtual machine was created.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. Power off the virtual machine.
3. From the Actions menu, select Edit Settings.
4. Select the **Virtual Hardware** tab in the dialog box displaying the settings.
5. From the **Add new device** drop-down menu, select **Network Adapter**.
   The New Network section is added to the list in the **Virtual Hardware** tab.
6. Expand the New Network section and connect the virtual machine to a port group.
   The virtual NIC does not use this port group for data traffic. The port group is used to extract the networking properties, for example VLAN tagging, to apply on the data traffic.
7. From the **Adapter type** drop-down menu, select **SR-IOV passthrough**.
8. From the **Physical function** drop-down menu, select the physical adapter to back the passthrough virtual machine adapter.
9. To allow changes in the MTU of packets from the guest operating system, use the **Guest OS MTU Change** drop-down menu.
10. Expand the Memory section, select **Reserve all guest memory (All locked)** and click **OK**.
    I/O memory management unit (IOMMU) must reach all virtual machine memory so that the passthrough device can access the memory by using direct memory access (DMA).
11. Power on the virtual machine.

When you power on the virtual machine, the ESXi host selects a free virtual function from the physical adapter and maps it to the SR-IOV passthrough adapter. The host validates all properties of the virtual machine adapter and the underlying virtual function against the settings of the port group to which the virtual machine belongs.

Networking Options for the Traffic Related to an SR-IOV Enabled Virtual Machine

In vSphere you can configure certain networking features on a virtual machine adapter that is associated virtual function (VF). Use settings for the switch, for the port group, or for a port depending on the type of the virtual switch (standard or distributed) that handles the traffic.

Table 189: Networking Options for a Virtual Machine Adapter That Uses a VF

Networking Option	Description
MTU size	Change the size of the MTU, for example, to enable jumbo frames.
Security policy for VF traffic	• If the guest operating system changes the initially set MAC address of a virtual machine network adapter that uses a VF, accept or drop incoming frames for the new address by setting the **MAC address changes** option. • Enable global promiscuous mode for virtual machine network adapters, including adapters that use VFs.
VLAN tagging mode	Configure VLAN tagging in the standard or distributed switch, and let the tagged traffic reach the virtual machines that are associated with VFs, that is, enable Virtual Guest Tagging (VGT).

Using an SR-IOV Physical Adapter to Handle Virtual Machine Traffic

In vSphere both the physical function (PF) and virtual functions (VFs) of an SR-IOV capable physical adapter can be configured to handle virtual machine traffic.

The PF of an SR-IOV physical adapter controls the VFs that virtual machines use, and can carry the traffic flowing through the standard or distributed switch that handles the networking of these SR-IOV enabled virtual machines.

The SR-IOV physical adapter works in different modes depending on whether it backs the traffic of the switch.

Mixed Mode

The physical adapter provides virtual functions to virtual machines attached to the switch and directly handles traffic from non SR-IOV virtual machines on the switch.

You can check whether an SR-IOV physical adapter is in mixed mode in the topology diagram of the switch. An SR-IOV physical adapter in mixed mode appears with the icon in the list of physical adapters for a standard switch or in the list of uplink group adapters for a distributed switch.

SR-IOV Only Mode

The physical adapter provides virtual functions to virtual machines connected to a virtual switch, but does not back traffic from non SR-IOV virtual machines on the switch.

To verify whether the physical adapter is in SR-IOV only mode, examine the topology diagram of the switch. In this mode, the physical adapter is in a separate list called External SR-IOV Adapters and appears with the icon.

Non SR-IOV Mode

The physical adapter is not used for traffic related to VF aware virtual machines. It handles traffic from non SR-IOV virtual machines only.

Related Links

View the Topology of a vSphere Distributed Switch on page 2191

Examine the organization of components that are connected to the distributed switch across the hosts in a vCenter Server.

View the Topology of a Host Proxy Switch on page 2192

Examine and reorganize the networking of the VMkernel and virtual machines that the vSphere Distributed Switch handles on a host.

View the Topology Diagram of a vSphere Standard Switch on page 2155
You can examine the structure and components of a vSphere Standard Switch by using its topology diagram.

Enabling SR-IOV by Using Host Profiles or an ESXCLI Command

You can configure the virtual functions on an ESXi host by using an ESXCLI command, or by using a host profile to set up multiple hosts simultaneously or to set up stateless hosts.

Enable SR-IOV in a Host Profile

For multiple hosts or a stateless host, you can configure the virtual functions of the physical NIC by using a host profile and apply the profile on a host by using Auto Deploy.

- Verify that the configuration of your environment supports SR-IOV. See SR-IOV Support.
- Create a host profile based on the SR-IOV capable host. See the *vSphere Host Profiles* documentation.

For information about running ESXi by using Auto Deploy with host profiles, see the *vCenter Server Installation and Setup* documentation.

You can also enable SR-IOV virtual functions on the host by using the `esxcli system module parameters set` vCLI command on the NIC driver parameter for virtual functions in accordance with the driver documentation. For more information about using ESXCLI commands, see *ESXCLI Concepts and Examples* documentation.

1. From the Home page, click **Host Profiles**.
2. Select the host profile from the list and click the **Configure** tab.
3. Click **Edit Host Profile** and expand the **General System Settings** node.
4. Expand **Kernel Module Parameter** and select the parameter of the physical function driver for creating virtual functions.
   For example, the parameter for the physical function driver of an Intel physical NIC is `max_vfs`.
5. In the **Value** text box, type a comma-separated list of valid virtual function numbers.

   Each list entry indicates the number of virtual functions that you want to configure for each physical function. A value of 0 ensures that SR-IOV is not enabled for that physical function.

   For example, if you have a dual port, set the value to *x*`,`*y* where *x* or *y* is the number of virtual functions you want to enable for a single port.

   If the target number of virtual functions on a single host is 30, you might have two dual port cards set to `0,10,10,10`.

   Note: The number of virtual functions supported and available for configuration depends on your system configuration.
6. Click **Finish**.
7. Remediate the host profile to the host as required.

The virtual functions appear in the PCI Devices list on the **Settings** tab for the host.

Associate a virtual function with a virtual machine adapter by using the SR-IOV passthrough network adapter type. See Assign a Virtual Function as SR-IOV Passthrough Adapter to a Virtual Machine.

Enable SR-IOV on a Host Physical Adapter by Using an ESXCLI Command

In certain troubleshooting situations or to configure hosts directly, you can run a console command on ESXi to create SR-IOV virtual functions on a physical adapter.

Install the vCLI package, deploy the vSphere Management Assistant (vMA) virtual machine, or use the ESXi Shell. See *Getting Started with ESXCLI*.

You can create SR-IOV virtual functions on the host by manipulating the NIC driver parameter for virtual functions in accordance with the driver documentation.

1. To create virtual functions by setting the parameter for virtual functions of the NIC driver, run the `esxcli system module parameters set` command at the command prompt.

   ```
   esxcli system module parameters set -m driver -p vf_param=w,x,y,z
   ```

   Where *driver* is the name of the NIC driver, and *vf_param* is the driver-specific parameter for creating the virtual function.

   You can use a comma-separated list to set values for the *vf_param* parameter, where each entry indicates the number of virtual functions for a port. A value of 0 ensures that SR-IOV is not enabled for that physical function.

   If you have two dual port NICs, you can set the value to *w*,*x*,*y*,*z* , where *w*,*x*,*y*, and *z* is the number of virtual functions you want to enable for a single port. For example, to create 30 virtual functions distributed on two dual port Intel cards by using the ixgbe driver, run the following command for the ixgbe driver and the `max_vfs` parameter:

   ```
   esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
   ```

2. Restart the host to create the virtual functions.

Associate a virtual function with a virtual machine adapter by using the SR-IOV passthrough network adapter type. See Assign a Virtual Function as SR-IOV Passthrough Adapter to a Virtual Machine.

Virtual Machine That Uses an SR-IOV Virtual Function Fails to Power On Because the Host Is Out of Interrupt Vectors

On an ESXi host, one or more virtual machines that use SR-IOV virtual functions (VFs) for networking are powered off.

On an ESXi host, one or more virtual machines that use SR-IOV virtual functions (VFs) for networking fail to power on if the total number of assigned virtual functions is close to the maximum number of VFs specified in the *vSphere Configuration Maximums* guide.

The virtual machine log file `vmware.log` contains the following message about the VF:

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

The VMkernel log file `vmkernel.log` contains the following messages about the VF assigned to the virtual machine:

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

The number of allocatable interrupt vectors scales up with the number of physical CPUs on an ESXi host. An ESXi host that has 32 CPUs can provide a total of 4096 interrupt vectors. When the host boots, devices on the host such as storage controllers, physical network adapters, and USB controllers consume a subset of the 4096 vectors. If these devices require more than 1024 vectors, the maximum number of potentially supported VFs is reduced.

When a virtual machine powers on and the guest operating system VF driver starts, interrupt vectors are consumed. If the required number of interrupt vectors is not available, the guest operating system shuts down unexpectedly without any error messages.

No rule presently exists to determine the number of interrupt vectors consumed or available on a host. This number depends on the hardware configuration of the host.

- To be able to power on the virtual machines, reduce the total number of VFs assigned to virtual machines on the host. For example, change the SR-IOV network adapter of a virtual machine to an adapter that is connected to a vSphere Standard Switch or vSphere Distributed Switch.

Related Links

vSphere and Virtual Function Interaction on page 2289

Virtual functions (VFs) are lightweight PCIe functions that contain all the resources necessary for data exchange but have a minimized set of configuration resources. Interaction between vSphere and VFs is limited.

Remote Direct Memory Access for Virtual Machines

vSphere 6.5 and later releases support remote direct memory access (RDMA) communication between virtual machines that have paravirtualized RDMA (PVRDMA) network adapters .

Overview of RDMA

RDMA allows direct memory access from the memory of one computer to the memory of another computer without involving the operating system or CPU. The transfer of memory is offloaded to the RDMA-capable Host Channel Adapters (HCA) . A PVRDMA network adapter provides remote direct memory access in a virtual environment.

Using RDMA in vSphere

In vSphere, a virtual machine can use a PVRDMA network adapter to communicate with other virtual machines that have PVRDMA devices. The virtual machines must be connected to the same vSphere Distributed Switch.

The PVRDMA device automatically selects the method of communication between the virtual machines . For virtual machines that run on the same ESXi host with or without a physical RDMA device, the data transfer is a memcpy between the two virtual machines. The physical RDMA hardware is not used in this case.

For virtual machines that reside on different ESXi hosts and that have a physical RDMA connection, the physical RDMA devices must be uplinks on the distributed switch. In this case, the communication between the virtual machines by way of PVRDMA uses the underlying physical RDMA devices.

For two virtual machines that run on different ESXi hosts, when at least one of the hosts does not have a physical RDMA device, the communication falls back to a TCP-based channel and the performance is reduced.

PVRDMA Support

vSphere 6.5 and later supports PVRDMA only in environments with a specific configuration.

Supported Configurations

To use PVRDMA in vSphere 6.5 or later, your environment must meet several configuration requirements.

Table 190: Supported Configurations for Using PVRDMA

Component	Requirements
vSphere	• ESXi host 6.5 or later. • vCenter Server 6.5 or later. • vSphere Distributed Switch.
Physical host	• Must be compatible with the ESXi release.

Component	Requirements
Host Channel Adapter (HCA)	• Must be compatible with the ESXi release. **Note:** Virtual machines that reside on different ESXi hosts require HCA to use RDMA. You must assign the HCA as an uplink for the vSphere Distributed Switch. PVRDMA does not support NIC teaming. The HCA must be the only uplink on the vSphere Distributed Switch. For virtual machines on the same ESXi hosts or virtual machines using the TCP-based fallback, the HCA is not required.
Virtual machine	• Virtual hardware version 13 or later.
Guest OS	• Linux (64-bit)

To verify that your physical hosts and HCAs are compatible with ESXi releases, see the *VMware Compatibility Guide*.

Note: Attempts to enable or configure unsupported features with PVRDMA might result in unexpected behavior in your environment.

Support for PVRDMA Namespaces

In releases previous to vSphere 7.0, PVRDMA virtualized public resource identifiers in the underlying hardware to guarantee that a physical resource can be allocated with the same public identifier when a virtual machine resumed operation following the use of vMotion to move it from one physical host server to another. To do this, PVRDMA distributed virtual to physical resource identifier translations to peers when creating a resource. This resulted in additional overhead that can be significant when creating large numbers of resources.

PVRDMA namespaces prevents these additional overheads by letting multiple virtual machines coexist without coordinating the assignment of identifiers. Each virtual machine is assigned an isolated identifier namespace on the RDMA hardware, such that any virtual machine can select its identifiers within the same range without conflicting with other virtual machines. The physical resource identifier no longer changes even after vMotion, so virtual to physical resource identifier translations are no longer necessary.

PVRDMA namespaces are enabled automatically on vSphere 7.0 and later with virtual machine hardware version 17 or later. The underlying hardware must also support PVRDMA namespaces. To learn how to enable PVRDMA namespaces on your environment's hardware, refer to the RDMA vendor documentation.

Support for PVRDMA Native Endpoints

PVRDMA native endpoints are supported in virtual machine hardware version 18 and later beginning with vSphere 7.0 Update 1 and later releases. PVRDMA native endpoints allow PVRDMA to communicate with non-PVRDMA endpoints. To use PVRDMA native endpoints, you must enable PVRDMA namespaces. To learn how to enable PVRDMA namespaces on your environment's specific hardware, refer to the RDMA vendor documentation.

You must configure the virtual machine to use PVRDMA native endpoints. See Configure a Virtual Machine to Use PVRDMA Native Endpoints.

Configure an ESXi Host for PVRDMA

Configure the VMkernel adapter and firewall rule of an ESXi host for PVRDMA communication.

Verify that your ESXi host meets the requirements for PVRDMA. See PVRDMA Support.

Tag a VMkernel Adapter for PVRDMA

Select a VMkernel adapter and enable it for PVRDMA communication.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Click the **Edit** button.
5. Locate `Net.PVRDMAVmknic`by using the filter text field.
6. Click the value field and enter the value of the VMkernel adapter that you want to use, for example vmk0.
7. Click **OK** .

Related Links

Enable the Firewall Rule for PVRDMA on page 2297
Enable the firewall rule for PVRDMA in the security profile of the ESXi host.

Enable the Firewall Rule for PVRDMA

Enable the firewall rule for PVRDMA in the security profile of the ESXi host.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Firewall**.
4. Click the **Edit** button.
5. Locate the pvrdma rule by using the filter text field.
6. Select the check box next to the pvrdma rule and click **OK**.

Related Links

Tag a VMkernel Adapter for PVRDMA on page 2297
Select a VMkernel adapter and enable it for PVRDMA communication.

Assign a PVRDMA Adapter to a Virtual Machine

To enable a virtual machine to exchange data by using RDMA, you must associate the virtual machine with a PVRDMA network adapter.

- Verify that the host on which the virtual machine is running is configured for RDMA. See Configure an ESXi Host for PVRDMA.
- Verify that the host is connected to a vSphere Distributed Switch.
- Verify that the virtual machine uses virtual hardware version 13 and above.

- Verify that the guest operating system is a Linux 64-bit distribution.

You can add up to ten PVRDMA network adapters to a virtual machine when using vSphere 7.0.2 and later.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. Power off the virtual machine.
3. From the Actions menu, select Edit Settings.
4. Select the **Virtual Hardware** tab in the dialog box displaying the settings.
5. From the **Add new device** drop-down menu, select **Network Adapter**.
   The New Network section is added to the list in the **Virtual Hardware** tab.
6. Expand the New Network section and connect the virtual machine to a distributed port group.
7. From the **Adapter type** drop-down menu, select PVRDMA.
8. Expand the **Memory** section, select **Reserve all guest memory (All locked)**, and click **OK**.
9. Power on the virtual machine.

Configure a Virtual Machine to Use PVRDMA Native Endpoints

PVRDMA native endpoints are available as an advanced virtual machine configuration.

Verify that your environment supports PVRDMA. See PVRDMA Support.

PVRDMA native endpoints are supported in virtual machine hardware version 18 and later beginning with vSphere 7.0 Update 1 and later releases. To use PVRDMA native endpoints, you must enable PVRDMA namespaces. To learn how to enable PVRDMA namespaces on your environment's specific hardware, refer to the vendor documentation.

You can use the vSphere Client to configure native endpoints or edit the virtual machine's VMX file. If editing the VMX file directly, add the parameter `vrdmax.nativeEndpointSupport = "TRUE"` , where *x* is the index of the PVRDMA adapter. The following procedure uses the vSphere Client to configure native endpoints.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click **VM Options**.
4. Expand **Advanced**.
5. Under Configuration Parameters, click the **Edit Configuration** button.
6. In the dialog box that appears, click **Add Row** to enter a new parameter and its value.
7. Enter the parameter `vrdmax.nativeEndpointSupport` , where *x* is the index of the PVRDMA adapter, and set the value to `TRUE`.
   The index *x* is the number of the PVRDMA adapter minus 1. For example, if the PVRDMA adapter you want to enable native endpoints with is labelled "Network Adapter 2," then the index is 1.

Network Requirements for RDMA over Converged Ethernet

RDMA over Converged Ethernet ensures low-latency, light-weight, and high-throughput RDMA communication over an Ethernet network. RoCE requires a network that is configured for lossless traffic of information at layer 2 alone or at both layer 2 and layer 3.

RDMA over Converged Ethernet (RoCE) is a network protocol that uses RDMA to provide faster data transfer for network-intensive applications. RoCE allows direct memory transfer between hosts without involving the hosts' CPUs.

There are two versions of the RoCE protocol. RoCE v1 operates at the link network layer (layer 2). RoCE v2 operates at the Internet network layer (layer 3) . Both RoCE v1 and RoCE v2 require a lossless network configuration. RoCE v1 requires a lossless layer 2 network, and RoCE v2 requires that both layer 2 and layer 3 are configured for lossless operation.

Lossless Layer 2 Network

To ensure lossless layer 2 environment, you must be able to control the traffic flows. Flow control is achieved by enabling global pause across the network or by using the Priority Flow Control (PFC) protocol defined by Data Center Bridging group (DCB). PFC is a layer 2 protocol that uses the class of services field of the 802.1Q VLAN tag to set individual traffic priorities. It puts on pause the transfer of packets towards a receiver in accordance with the individual class of service priorities. This way, a single link carries both lossless RoCE traffic and other lossy, best-effort traffic. With traffic flow congestion, important lossy traffic can be affected. To isolate different flows from one another, use RoCE in a PFC priority-enabled VLAN.

Lossless Layer 3 Network

RoCE v2 requires that lossless data transfer is preserved at layer 3 routing devices. To enable the transfer of layer 2 PFC lossless priorities across layer 3 routers, configure the router to map the received priority setting of a packet to the corresponding Differentiated Serviced Code Point (DSCP) QoS setting that operates at layer 3. The transferred RDMA packets are marked with layer 3 DSCP, layer 2 Priority Code Points (PCP) or with both. To extract priority information from the packet routers use either DSCP or PCP. In case PCP is used, the packet must be VLAN-tagged and the router must copy the PCP bits of the tag and forward them to the next network. If the packet is marked with DSCP, the router must keep the DSCP bits unchanged.

Like RoCE v1, RoCE v2 must run on a PFC priority-enabled VLAN.

Note: Do not team RoCE NICs, if you intend to use RDMA on those NICs.

For vendor-specific configuration information, refer to the official documentation of the respective device or the switch vendor.

Configure Remote Direct Memory Access Network Adapters

You can install a remote direct memory access (RDMA) network adapter on your ESXi hosts. Once installed, you can use the vSphere Client to view the RDMA adapter and its corresponding network adapter, and configure its VMkernel binding.

Install an RDMA-capable adapter on your ESXi host. For example, Mellanox Technologies MT27700 Family ConnectX-4.

RDMA provides direct memory access from the memory of one host to the memory of another host without involving the remote operating system and CPU. This boosts network and host performance with lower latency, lower CPU load, and faster bandwidth.

View RDMA Capable Network Adapter

ESXi supports RDMA capable network adapters. After you install such an adapter on your ESXi host, the vSphere Client displays its two components, the RDMA adapter, and a physical network adapter.

Install a RDMA-capable adapter that supports RDMA (RoCE v2) on your ESXi host. For example, Mellanox Technologies MT27700 Family ConnectX-4.

You can use the vSphere Client to view the RDMA adapter and its corresponding network adapter.

1. On your ESXi host, install a RDMA-capable adapter that supports RDMA (RoCE v2).

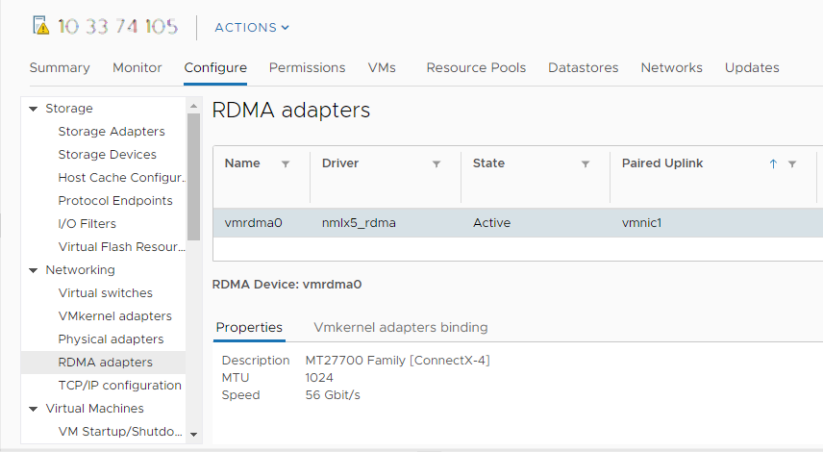
   The host discovers the adapter and the vSphere Client displays its two components, an RDMA adapter, and a physical network adapter.

2. Navigate to the host.

3. Under **Networking**, click **RDMA adapters**.

   In this example, the RDMA adapter appears on the list as `vmrdma0`. The **Paired Uplink** column displays the network component as the `vmnic1` physical network adapter.

   Figure 58: RDMA adapters installed on an ESXi host in a vSphere environment.



4. To verify the description of the adapter, select the RDMA adapter from the list, and click the **Properties** tab.

Configure Remote Direct Memory Access Network Adapters

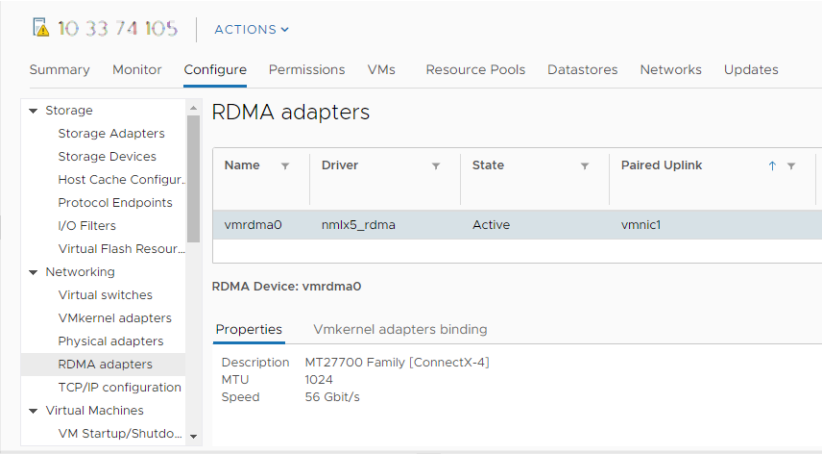
You can install a remote direct memory access (RDMA) network adapter and configure its VMkernel binding.

1. Install an RDMA-capable adapter that supports RDMA (RoCE v2) on your ESXi host.

   The host discovers the adapter and the vSphere Client displays its two components, an RDMA adapter and a physical network adapter.

2. In the vSphere Client, verify that the RDMA adapter is discovered by your host.
   a) Navigate to the host.
   b) Click the **Configure** tab.
   c) Under **Networking**, click **RDMA adapters**.

      In this example, the RDMA adapter appears on the list as `vmrdma0`. The **Paired Uplink** column displays the network component as the `vmnic1` physical network adapter.



   d) To verify the description of the adapter, select the RDMA adapter from the list, and click the **Properties** tab.

3. Configure VMkernel binding for the RDMA adapter.

   In the configuration, you can use a vSphere standard switch or a vSphere Distributed Switch. The following steps use the standard switch as an example.

   a) Create a vSphere standard switch and add the network component to the switch.

      Note: Make sure to select the physical network adapter that corresponds to the RDMA adapter. In this example, it is the `vmnic1` adapter.

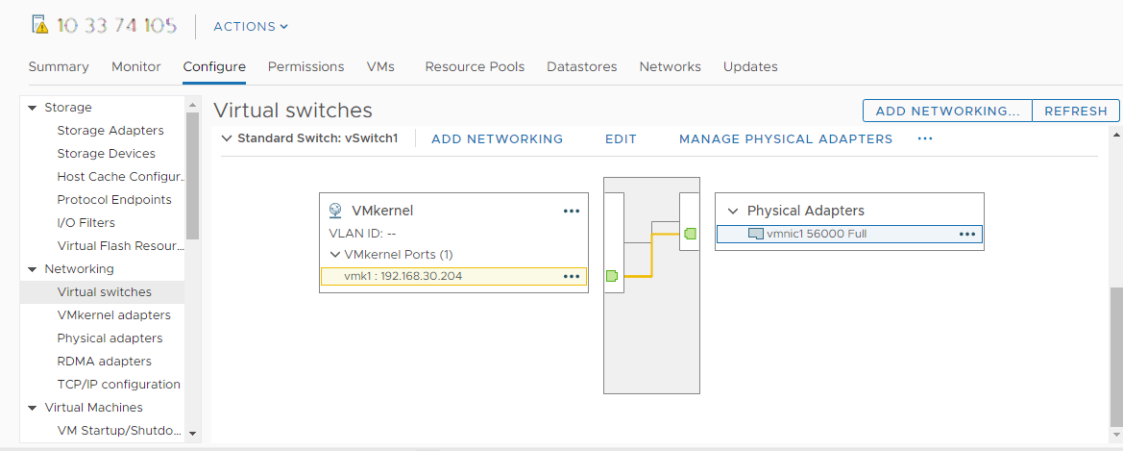
For information about creating the switch, see Create a vSphere Standard Switch or Create a vSphere Distributed Switch.

b) Add a VMkernel adapter to the vSphere standard switch that you created.

Assign an appropriate static IPv4 or IPv6 address to the VMkernel adapter, so that your RDMA adapter can discover the NVMe over RDMA target.

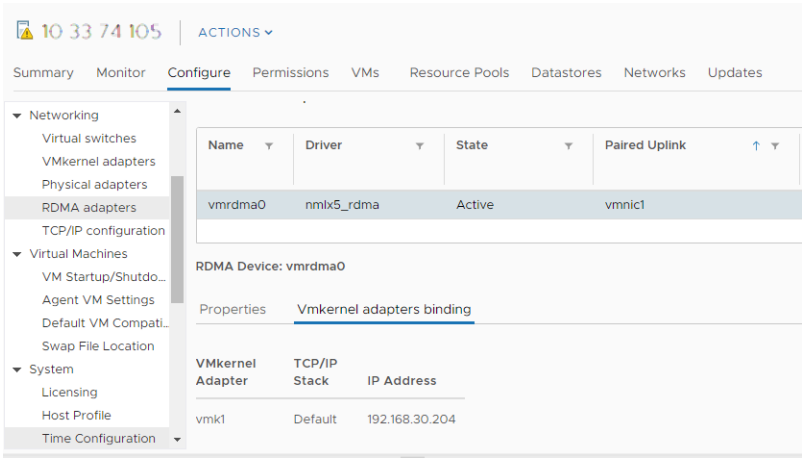
For information about adding the VMkernel adapter, see Setting Up VMkernel Networking.

The illustration shows that the physical network adapter and the VMkernel adapter are connected to the vSphere standard switch. Through this connection, the RDMA adapter is bound to the VMkernel adapter.



4. Verify the VMkernel binding configuration for the RDMA adapter.
   a) Navigate to the RDMA adapter.
   b) Click the **VMkernel adapters binding** tab and verify that the associated VMkernel adapter appears on the page.

   In this example, the `vmrdma0` RDMA adapter is paired to the `vmnic1` network adapter and is connected to the `vmk1` VMkernel adapter.



You can use the RDMA network component of the adapter for such storage configurations as iSER or NVMe over RDMA. To learn more, see the *vSphere Storage* documentation.

What are Jumbo Frames

Jumbo frames let ESXi hosts send larger frames out onto the physical network. The network must support jumbo frames end-to-end that includes physical network adapters, physical switches, and storage devices.

Before enabling jumbo frames, check with your hardware vendor to ensure that your physical network adapter supports jumbo frames.

You can enable jumbo frames on a vSphere distributed switch or vSphere standard switch by changing the maximum transmission unit (MTU) to a value greater than 1280 bytes. With vCenter Server 7.0 Update 3, you can set the size of the maximum transmission unit (MTU) on a vSphere Distributed Switch to up to 9190 bytes to support switches with larger packet sizes.

Enable Jumbo Frames on a vSphere Distributed Switch

Enable jumbo frames for the entire traffic that passes through a vSphere Distributed Switch.

Important: When you change the MTU size of a vSphere Distributed Switch, the physical NICs that are assigned as uplinks are brought down and up again. This causes a short network outage of between 5 to 10 milliseconds for virtual machines or services that are using the uplinks.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and select **Properties**.
3. Click **Edit**.
4. Click **Advanced** and set the **MTU** property to a value greater than 1500 bytes.
   You cannot set the MTU size to a value greater than 9190 bytes.
5. Click **OK**.

Enable Jumbo Frames on a vSphere Standard Switch

Enable jumbo frames for all traffic through a vSphere Standard Switch on a host.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select a standard switch from the virtual switch table and click **Edit settings**.
4. In the **Properties** section, set the **MTU** property to a value greater than 1500 bytes.
   You can increase the MTU size up to 9000 bytes.
5. Click **OK**.

Enable Jumbo Frames for a VMkernel Adapter

Jumbo frames reduce the CPU load caused by transferring data. Enable jumbo frames on a VMkernel adapter by changing the maximum transmission units (MTU) of the adapter.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **VMkernel adapters**.
3. Select a VMkernel adapter from the adapter table.
   The properties of the adapter appear.
4. Click **Edit**.
5. On the Port properties page, set the **MTU** property to a value greater than 1500.
   You can increase the MTU size up to 9000 bytes.

6. Click **OK**.

Enable Jumbo Frame Support on a Virtual Machine

Enabling jumbo frame support on a virtual machine requires an enhanced VMXNET adapter for that virtual machine.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. From the Actions menu, select Edit Settings.
3. Select the **Virtual Hardware** tab in the dialog box displaying the settings.
4. Expand the **Network adapter** section. Record the network settings and MAC address that the network adapter is using.
5. Click the times-circle button to remove the network adapter from the virtual machine.
6. From the **Add new device** drop-down menu, select **Network Adapter**.
   The New Network section is added to the list in the Virtual Hardware tab.
7. Expand the New Network section.
8. From the **Adapter Type** drop-down menu, select **VMXNET 2 (Enhanced)** or **VMXNET 3**.
9. Set the network settings to the ones recorded for the old network adapter.
10. Set the **MAC Address** to **Manual**, and type the MAC address that the old network adapter was using.
11. Click **OK**.

- Check that the enhanced VMXNET adapter is connected to a standard switch or to a distributed switch with jumbo frames enabled.
- Inside the guest operating system, configure the network adapter to allow jumbo frames. See the documentation of your guest operating system.
- Configure all physical switches and any physical or virtual machines to which this virtual machine connects to support jumbo frames.

TCP Segmentation Offload

Use TCP Segmentation Offload (TSO) in VMkernel network adapters and virtual machines to improve the network performance in workloads that have severe latency requirements.

TSO on the transmission path of physical network adapters, and VMkernel and virtual machine network adapters improves the performance of ESXi hosts by reducing the overhead of the CPU for TCP/IP network operations. When TSO is enabled, the network adapter divides larger data chunks into TCP segments instead of the CPU. The VMkernel and the guest operating system can use more CPU cycles to run applications.

To benefit from the performance improvement that TSO provides, enable TSO along the data path on an ESXi host including physical network adapters, VMkernel and guest operating system. By default, TSO is enabled in the VMkernel of the ESXi host , and in the VMXNET 2 and VMXNET 3 virtual machine adapters.

For information about the location of TCP packet segmentation in the data path, see VMware Knowledge Base article Understanding TCP Segmentation Offload (TSO) and Large Receive Offload (LRO) in a VMware environment.

Enable or Disable Software TSO in the VMkernel

If a physical network adapter experiences problems with TSO, you can temporarily enable the software simulation of TSO in the VMkernel until you troubleshoot the problems.

Run these `esxcli network nic software set` console commands to enable or disable the software simulation of TSO in the VMkernel.

- Enable the software simulation of TSO in the VMkernel.

  `esxcli network nic software set --ipv4tso=1 -n vmnic`*X*`esxcli network nic software set --ipv6tso=1 -n vmnic`*X*

- Disable the software simulation of TSO in the VMkernel.

  `esxcli network nic software set --ipv4tso=0 -n vmnic`*X*`esxcli network nic software set --ipv6tso=0 -n vmnic`*X*

where *X* in vmnic*X* represents the number of the NIC ports on the host.

The configuration change persists across host reboots.

Determine Whether TSO Is Supported on the Physical Network Adapters on an ESXi Host

Examine whether a physical network adapter offloads TCP/IP packet segmentation when you estimate the networking performance on a host that runs latency-sensitive workloads. If a physical network adapter supports TSO, then TSO is enabled by default.

Run the following console command to determine whether TSO is enabled on the physical network adapters on a host.

```
esxcli network nic tso get
```

Enable or Disable TSO on an ESXi Host

Enable TCP Segmentation Offload (TSO) on the transmission path to have the NIC divide larger data chunks into TCP segments. Disable TSO to have CPU perform TCP segmentation.

By default, a host uses hardware TSO if its physical adapters support it.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Edit the value of the `Net.UseHwTSO` parameter for IPv4 and of `Net.UseHwTSO6` for IPv6.
   - To enable TSO, set `Net.UseHwTSO` and `Net.UseHwTSO6` to `1`.
   - To disable TSO, set `Net.UseHwTSO` and `Net.UseHwTSO6` to `0`.
5. Click **OK** to apply the changes.
6. To reload the driver module of the physical adapter, run the `esxcli system module set` console command in the ESXi Shell on the host.
   a) To disable the driver, run the `esxcli system module set` command with the --enabled false option.

      `esxcli system module set--enabled false--module`*nic_driver_module*

   b) To enable the driver, run the `esxcli system module set` command with the --enabled true option.

      `esxcli system module set--enabled true--module`*nic_driver_module*

If a physical adapter does not support hardware TSO, the VMkernel segments large TCP packets coming from the guest operating system and sends them to the adapter.

Determine Whether TSO Is Enabled on an ESXi Host

Examine whether hardware TSO is enabled in the VMkernel when you estimate the networking performance on a host that runs latency-sensitive workloads. By default, hardware TSO is enabled on an ESXi host.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Examine the value of the `Net.UseHwTSO` and `Net.UseHwTSO6` parameters.
   `Net.UseHwTSO` shows the TSO state for IPv4, and `Net.UseHwTSO6` for IPv6. TSO is enabled if the property is set to 1.

Manage TSO on a Linux Virtual Machine

Activate TSO support on the network adapter of a Linux virtual machine so that the guest operating system redirects TCP packets that need segmentation to the VMkernel.

- Verify that ESXi supports the Linux guest operating system.
  See the *VMware Compatibility Guide* documentation.
- Verify that the network adapter on the Linux virtual machine is VMXNET2 or VMXNET3.

In a terminal window on the Linux guest operating system, to activate or deactivate TSO, run the `ethtool` command with the -K and tso options.

- To activate TSO, run the following command:
  `ethtool-K ethYtsoon`
- To deactivate TSO, run the following command:
  `ethtool-K ethYtsooff`

where *Y* in eth*Y* is the sequence number of the NIC in the virtual machine.

Manage TSO on a Windows Virtual Machine

By default, TSO is activated on a Windows virtual machine on VMXNET2 and VXMNET3 network adapters. For performance reasons, you might want to deactivate TSO.

- Verify that ESXi supports the Windows guest operating system. See the *VMware Compatibility Guide* documentation.
- Verify that the network adapter on the Windows virtual machine is VMXNET2 or VMXNET3.

1. In the Network and Sharing Center on the Windows control panel, click the name of the network adapter.
2. Click its name.
   A dialog box displays the status of the adapter.
3. Click **Properties**, and beneath the network adapter type, click **Configure**.
4. On the **Advanced** tab, set the **Large Send Offload V2 (IPv4)** and **Large Send Offload V2 (IPv6)** properties to **Enabled** or **Disabled**.
5. Click **OK**.
6. Restart the virtual machine.

Large Receive Offload

Use Large Receive Offload (LRO) to reduce the CPU overhead for processing packets that arrive from the network at a high rate.

LRO reassembles incoming network packets into larger buffers and transfers the resulting larger but fewer packets to the network stack of the host or virtual machine. The CPU has to process fewer packets than when LRO is disabled, which reduces its utilization for networking especially in the case of connections that have high bandwidth.

To benefit from the performance improvement of LRO, enable LRO along the data path on an ESXi host including VMkernel and guest operating system. By default, LRO is enabled in the VMkernel and in the VMXNET3 virtual machine adapters.

For information about the location of TCP packet aggregation in the data path, see VMware Knowledge Base article Understanding TCP Segmentation Offload (TSO) and Large Receive Offload (LRO) in a VMware environment.

Manage Hardware LRO for All VMXNET3 Adapters on an ESXi Host

Activate the hardware capabilities of host physical adapters to aggregate incoming TCP packets for VXMNET3 VM adapters by using the LRO technology instead of consuming resources for assembling in the guest operating system.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Edit the value of the `Net.Vmxnet3HwLRO` parameter.
   - To activate hardware LRO, set `Net.Vmxnet3HwLRO` to `1`.
   - To deactivate hardware LRO, set `Net.Vmxnet3HwLRO` to `0`.
5. Click **OK** to apply the changes.

Manage Software LRO for All VMXNET3 Adapters on an ESXi Host

Use software LRO in the VMkernel backend of VMXNET3 adapters to improve networking performance of virtual machines if the host physical adapters do not support hardware LRO.

vSphere supports software LRO for both IPv4 and IPv6 packets.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Edit the value of the `Net.Vmxnet3SwLRO` parameter for VMXNET3 adapters.
   - To activate software LRO, set `Net.Vmxnet3SwLRO` to 1.
   - To deactivate software LRO, set `Net.Vmxnet3SwLRO` to 0.
5. Click **OK** to apply the changes.

Determine Whether LRO Is Enabled for VMXNET3 Adapters on an ESXi Host

Examine the status of LRO on an ESXi when you estimate the networking performance on a host that runs latency-sensitive workloads.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Examine the value of the LRO parameters for VMXNET2 and VMXNET3.
   - For hardware LRO, examine the `Net.Vmxnet3HwLRO` parameter. If it is equal to 1, hardware LRO is enabled.
   - For software LRO, examine the `Net.Vmxnet3SwLRO` parameter. If it is equal to 1, hardware LRO is enabled.

Change the Size of the LRO Buffer for VMXNET 3 Adapters

You can change the size of the buffer for packet aggregation for virtual machine connections through VMXNET 3 network adapters. Increase the buffer size to reduce the number of TCP acknowledgments and improve efficiency in workloads.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Enter a value between 1 and 65535 for the `Net.VmxnetLROMaxLength` parameter to set the LRO buffer size in bytes.

   By default the size of the LRO buffer is equal to 32000 bytes.

Enable or Disable LRO for All VMkernel Adapters on an ESXi Host

Use LRO in the VMkernel network adapters on an ESXi host to improve the networking performance for incoming infrastructure traffic.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Edit the value of the `Net.TcpipDefLROEnabled` parameter.
   - To enable LRO for the VMkernel network adapters on the host, set `Net.TcpipDefLROEnabled` to `1`.
   - To disable software LRO for the VMkernel network adapters on the host, set `Net.TcpipDefLROEnabled` to `0`.
5. Click **OK** to apply the changes.

Change the Size of the LRO Buffer for VMkernel Adapters

You can change the size of the buffer for packet aggregation for VMkernel connections. Increase the buffer size to reduce the number of TCP acknowledgments and improve efficiency in the VMkernel.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System**.
3. Click **Advanced System Settings**.
4. Enter a value between 1 and 65535 for the `Net.TcpipDefLROMaxLength` parameter to set the LRO buffer size in bytes.

   By default the size of the LRO buffer is equal to 32768 bytes.

Manage LRO on a VMXNET3 Adapter on a Linux Virtual Machine

If LRO is enabled for VMXNET3 adapters on the host, activate LRO support on a network adapter on a Linux virtual machine to ensure that the guest operating system does not spend resources to aggregate incoming packets into larger buffers.

Verify that the Linux kernel is 2.6.24 and later.

In a terminal window on the Linux guest operating system, run the `ethtool` command with the -K and lro options.

- To activate LRO, run the following command:
  ```
  ethtool-K ethYlroon
  ```
  where *Y* in eth*Y* is the sequence number of the NIC in the virtual machine.
- To deactivate LRO, run the following command:
  ```
  ethtool-K ethYlrooff
  ```
  where *Y* in eth*Y* is the sequence number of the NIC in the virtual machine.

Enable or Disable LRO on a VMXNET3 Adapter on a Windows Virtual Machine

If LRO is enabled for VMXNET3 adapters on the host, activate LRO support on a network adapter on a Windows virtual machine to ensure that the guest operating system does not spend resources to aggregate incoming packets into larger buffers.

- Verify that the virtual machine runs Windows Server 2012 and later or Windows 8 and later.
- Verify that the virtual machine compatibility is ESXi 6.0 and later.
- Verify that the version of the VMXNET3 driver installed on the guest operating system is 1.6.6.0 and later.
- Verify that LRO is enabled globally on a virtual machine that runs Windows Server 2012 and later or Windows 8 and later. See Enable LRO Globally on a Windows Virtual Machine.

On Windows, the LRO technology is also referred to as Receive Side Coalescing (RSC).

1. In the **Network and Sharing Center** of the guest operating system's Control Panel, click the name of the network adapter.

   A dialog box displays the status of the adapter.
2. Click **Properties**, and under the VMXNET3 network adapter type, click **Configure**.
3. On the **Advanced** tab, set both **Recv Segment Coalescing (IPv4)** and **Recv Segment Coalescing (IPv6)** to **Enabled** or **Disabled**.
4. Click **OK**.

Enable LRO Globally on a Windows Virtual Machine

To use Large Receive Offload (LRO) on a VMXNET3 adapter on a virtual machine that runs Windows 8 and later or Windows Server 2012 and later, you must enable LRO globally on the guest operating system. On Windows, the LRO technology is also referred to as Receive Side Coalescing (RSC).

1. To verify whether LRO is disabled globally on a Windows 8 and later or Windows Server 2012 guest OS, run the `netsh int tcp show global` command at the command prompt.
   ```
   netsh int tcp show global
   ```
   The command displays the status of the global Transmission Control Protocol (TCP) parameters that are set on the Windows 8.x OS.
   ```
   TCP Global Parameters
   ----------------------------------------------
   ```

```
Receive-Side Scaling State          : enabled
Chimney Offload State               : disabled
NetDMA State                        : disabled
Direct Cache Access (DCA)           : disabled
Receive Window Auto-Tuning Level    : normal
Add-On Congestion Control Provider  : none
ECN Capability                      : disabled
RFC 1323 Timestamps                 : disabled
Initial RTO                         : 3000
Receive Segment Coalescing State    : disabled
```

If LRO is globally disabled on the Windows 8 and later or Windows Server 2012 machine, the Receive Segment Coalescing State property appears as disabled.

2. To enable LRO globally on the Windows OS, run the `netsh int tcp set global` command at the command prompt:

   ```
   netsh int tcp set global rsc=enabled
   ```

Enable LRO for the VMXNET3 adapter on the Windows 8 and later or Windows Server 2012 virtual machine. See Enable or Disable LRO on a VMXNET3 Adapter on a Windows Virtual Machine.

NetQueue and Networking Performance

NetQueue takes advantage of the ability of some network adapters to deliver network traffic to the system in multiple receive queues that can be processed separately, allowing processing to be scaled to multiple CPUs, improving receive-side networking performance.

To use Rx queues effectively in the physical NICs by managing the vNIC and the VMkernel adapter filters, the NetQueue balancer in ESXi uses load balancing algorithms.

You can activate or deactivate different types of Rx queues. For more information, see the `esxcli network nic queue loadbalancer set` command in the *ESXCLI Reference* documentation.

Activate NetQueue on a Host

NetQueue is enabled by default. To use NetQueue after it has been deactivated, you must activate it again.

1. In the ESXi Shell on the host, use the following command:

   ```
   esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
   ```

2. To configure the NIC driver to use NetQueue, use the `esxcli module parameters set` command .
   To configure the driver with eight receive queues.on a dual-port Emulex NIC, run this ESXCLI command.

   ```
   esxcli system module parameters set -m tg3 -p force_netq=8,8
   ```

3. Reboot the host.

Deactivate NetQueue on a Host

NetQueue is activated by default.

Familiarize yourself with the information on configuring NIC drivers in *Getting Started with ESXCLI*.

1. In the ESXCLI, use the following command depending on the host version:

   ```
   esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
   ```

2. To deactivate NetQueue on the NIC driver, use the `esxcli module parameters set` command.
   To configure the driver with one receive queues, run the ESXCLI commands on a dual-port Emulex NIC.

   ```
   esxcli system module parameters set -m tg3 -p force_netq=1,1
   ```

3. Reboot the host.

vSphere Network I/O Control

Use vSphere Network I/O Control to allocate network bandwidth to business-critical applications and to resolve situations where several types of traffic compete for common resources.

About vSphere Network I/O Control Version 3

vSphere Network I/O Control version 3 introduces a mechanism to reserve bandwidth for system traffic based on the capacity of the physical adapters on a host. It enables fine-grained resource control at the VM network adapter level similar to the model that you use for allocating CPU and memory resources..

Version 3 of the Network I/O Control feature offers improved network resource reservation and allocation across the entire switch.

Models for Bandwidth Resource Reservation

Network I/O Control version 3 supports separate models for resource management of system traffic related to infrastructure services, such as vSphere Fault Tolerance, and of virtual machines.

The two traffic categories have different nature. System traffic is strictly associated with an ESXi host. The network traffic routes change when you migrate a virtual machine across the environment. To provide network resources to a virtual machine regardless of its host, in Network I/O Control you can configure resource allocation for virtual machines that is valid in the scope of the entire distributed switch.

Bandwidth Guarantee to Virtual Machines

Network I/O Control version 3 provisions bandwidth to the network adapters of virtual machines by using constructs of shares, reservation and limit. Based on these constructs, to receive sufficient bandwidth, virtualized workloads can rely on admission control in vSphere Distributed Switch, vSphere DRS and vSphere HA. See Admission Control for Virtual Machine Bandwidth.

Availability of Features

SR-IOV is not available for virtual machines configured to use Network I/O Control version 3.

Enable Network I/O Control on a vSphere Distributed Switch

Enable network resource management on a vSphere Distributed Switch to guarantee minimum bandwidth to system traffic for vSphere features and to virtual machine traffic.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. From the **Actions** menu, select **Settings** > **Edit Settings**.
3. From the **Network I/O Control** drop-down menu, select **Enable**.
4. Click **OK**.

When enabled, the model that Network I/O Control uses to handle bandwidth allocation for system traffic and virtual machine traffic is based on the Network I/O Control version that is active on the distributed switch. See About vSphere Network I/O Control Version 3.

Bandwidth Allocation for System Traffic

You can configure Network I/O Control to allocate certain amount of bandwidth for traffic generated by vSphere Fault Tolerance, vSphere vMotion, and so on.

You can use Network I/O Control on a distributed switch to configure bandwidth allocation for the traffic that is related to the main vSphere features:

- Management
- Fault Tolerance
- NFS
- vSAN
- vMotion
- vSphere Replication
- vSphere Data Protection Backup
- Virtual machine

vCenter Server propagates the allocation from the distributed switch to each physical adapter on the hosts that are connected to the switch.

Bandwidth Allocation Parameters for System Traffic

By using several configuration parameters Network I/O Control allocates bandwidth to traffic from basic vSphere system features.

Table 191: Allocation Parameters for System Traffic

Parameter for Bandwidth Allocation	Description
Shares	Shares, from 1 to 100, reflect the relative priority of a system traffic type against the other system traffic types that are active on the same physical adapter. The amount of bandwidth available to a system traffic type is determined by its relative shares and by the amount of data that the other system features are transmitting.
Reservation	The minimum bandwidth, in Mbps, that must be guaranteed on a single physical adapter. The total bandwidth reserved among all system traffic types cannot exceed 75 percent of the bandwidth that the physical network adapter with the lowest capacity can provide. Reserved bandwidth that is unused becomes available to other types of system traffic. However, Network I/O Control does not redistribute the capacity that system traffic does not use to virtual machine placement.
Limit	The maximum bandwidth, in Mbps or Gbps, that a system traffic type can consume on a single physical adapter.

Related Links

Example Bandwidth Reservation for System Traffic on page 2313

The capacity of the physical adapters determines the bandwidth that you guarantee. According to this capacity, you can guarantee minimum bandwidth to a system feature for its optimal operation.

Configure Bandwidth Allocation for System Traffic on page 2313

Assign bandwidth for host management, virtual machines, NFS storage, vSphere vMotion, vSphere Fault Tolerance, vSAN, and vSphere Replication on the physical adapters that are connected to a vSphere Distributed Switch.

Example Bandwidth Reservation for System Traffic

The capacity of the physical adapters determines the bandwidth that you guarantee. According to this capacity, you can guarantee minimum bandwidth to a system feature for its optimal operation.

For example, on a distributed switch that is connected to ESXi hosts with 10 GbE network adapters, you might configure reservation to guarantee 1 Gbps for management through vCenter Server, 1 Gbps for vSphere Fault Tolerance, 1 Gbps for vSphere vMotion traffic, and 0.5 Gbps for virtual machine traffic. Network I/O Control allocates the requested bandwidth on each physical network adapter. You can reserve no more than 75 percent of the bandwidth of a physical network adapter, that is, no more than 7.5 Gbps.

You might leave more capacity unreserved to let the host allocate bandwidth dynamically according to shares, limits, and use, and to reserve only bandwidth that is enough for the operation of a system feature.

Related Links

Bandwidth Allocation Parameters for System Traffic on page 2312
By using several configuration parameters Network I/O Control allocates bandwidth to traffic from basic vSphere system features.

Configure Bandwidth Allocation for System Traffic on page 2313
Assign bandwidth for host management, virtual machines, NFS storage, vSphere vMotion, vSphere Fault Tolerance, vSAN, and vSphere Replication on the physical adapters that are connected to a vSphere Distributed Switch.

Configure Bandwidth Allocation for System Traffic

Assign bandwidth for host management, virtual machines, NFS storage, vSphere vMotion, vSphere Fault Tolerance, vSAN, and vSphere Replication on the physical adapters that are connected to a vSphere Distributed Switch.

- Verify that vSphere Distributed Switch is version 6.5.0 and later.
- Verify that Network I/O Control on the switch is version 3.

To enable bandwidth allocation for virtual machines by using Network I/O Control, configure the virtual machine system traffic. The bandwidth reservation for virtual machine traffic is also used in admission control. When you power on a virtual machine, admission control verifies that enough bandwidth is available.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Resource Allocation**.
3. Click **System Traffic**.
   You see the bandwidth allocation for the types of system traffic.
4. Select the traffic type according to the vSphere feature that you want to provision and click **Edit**.
   The network resource settings for the traffic type appear.
5. From the **Shares** drop-down menu, edit the share of the traffic in the overall flow through a physical adapter.

   Network I/O Control applies the configured shares when a physical adapter is saturated.

   You can select an option to set a pre-defined value, or select **Custom** and type a number from 1 to 100 to set another share.
6. In the **Reservation** text box, enter a value for the minimum bandwidth that must be available for the traffic type.
   The total reservation for system traffic must not exceed 75% of the bandwidth supported by the physical adapter with the lowest capacity of all adapters connected to the distributed switch.

7. In the **Limit** text box, set the maximum bandwidth that system traffic of the selected type can use.
8. Click **OK** to apply the allocation settings.

vCenter Server propagates the allocation from the distributed switch to the host physical adapters that are connected to the switch.

Related Links

Bandwidth Allocation Parameters for System Traffic on page 2312
By using several configuration parameters Network I/O Control allocates bandwidth to traffic from basic vSphere system features.

Example Bandwidth Reservation for System Traffic on page 2313
The capacity of the physical adapters determines the bandwidth that you guarantee. According to this capacity, you can guarantee minimum bandwidth to a system feature for its optimal operation.

Bandwidth Allocation for Virtual Machine Traffic

Version 3 of Network I/O Control lets you configure bandwidth requirements for individual virtual machines. You can also use network resource pools where you can assign a bandwidth quota from the aggregated reservation for the virtual machine traffic and then allocate bandwidth from the pool to individual virtual machines.

About Allocating Bandwidth for Virtual Machines

Network I/O Control allocates bandwidth for virtual machines by using two models: allocation across the entire vSphere Distributed Switch based on network resource pools and allocation on the physical adapter that carries the traffic of a virtual machine.

Network Resource Pools

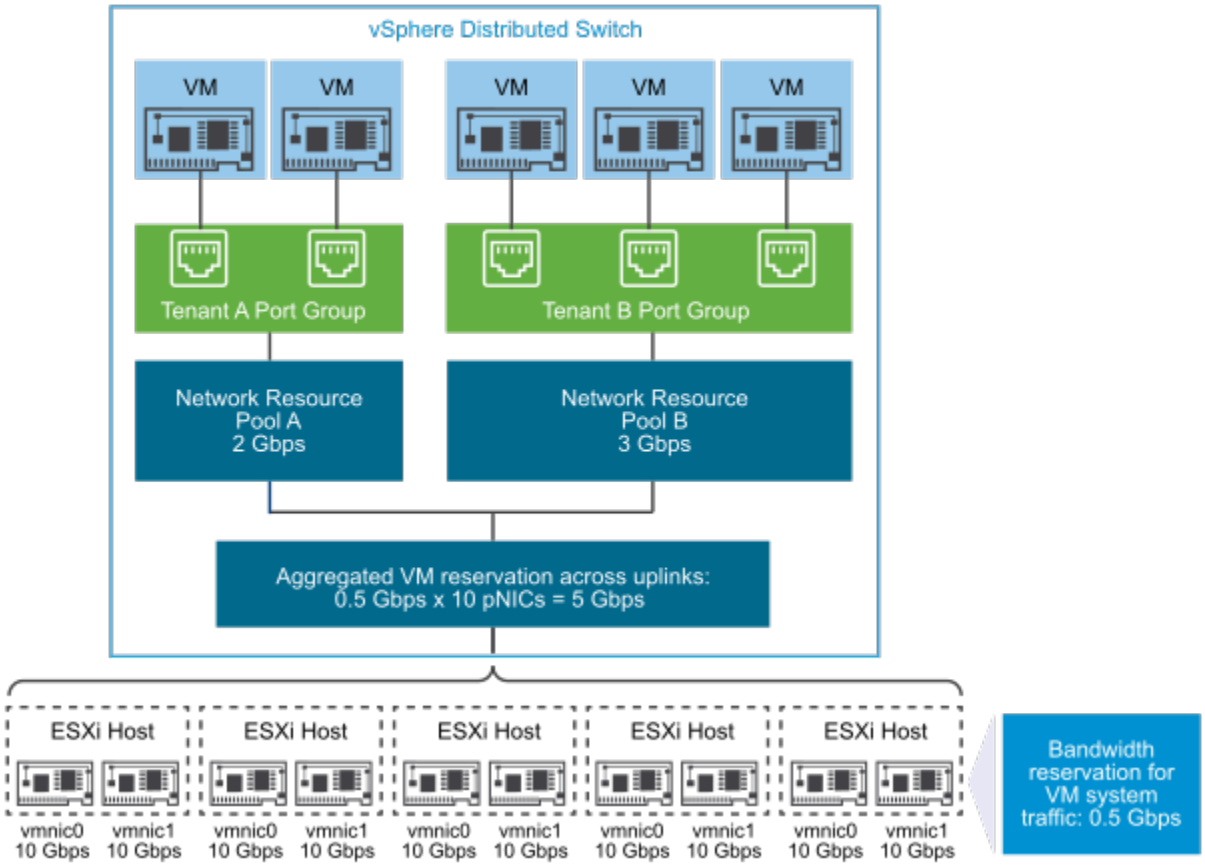
A network resource pool represents a part of the aggregated bandwidth that is reserved for the virtual machine system traffic on all physical adapters connected to the distributed switch.

For example, if the virtual machine system traffic has 0.5 Gbps reserved on each 10 GbE uplink on a distributed switch that has 10 uplinks, then the total aggregated bandwidth available for VM reservation on this switch is 5 Gbps. Each network resource pool can reserve a quota of this 5 Gbps capacity.

The bandwidth quota that is dedicated to a network resource pool is shared among the distributed port groups associated with the pool. A virtual machine receives bandwidth from the pool through the distributed port group the VM is connected to.

By default, distributed port groups on the switch are assigned to a network resource pool, called default, whose quota is not configured.

Figure 59: Bandwidth Aggregation for Network Resource Pools Across the Uplinks of a vSphere Distributed Switch



Defining Bandwidth Requirements for a Virtual Machine

You allocate bandwidth to an individual virtual machine similarly to allocating CPU and memory resources. Network I/O Control version 3 provisions bandwidth to a virtual machine according to shares, reservation, and limits that are defined for a network adapter in the VM hardware settings. The reservation represents a guarantee that the traffic from the virtual machine can consume at least the specified bandwidth. If a physical adapter has more capacity, the virtual machine may use additional bandwidth according to the specified shares and limit.

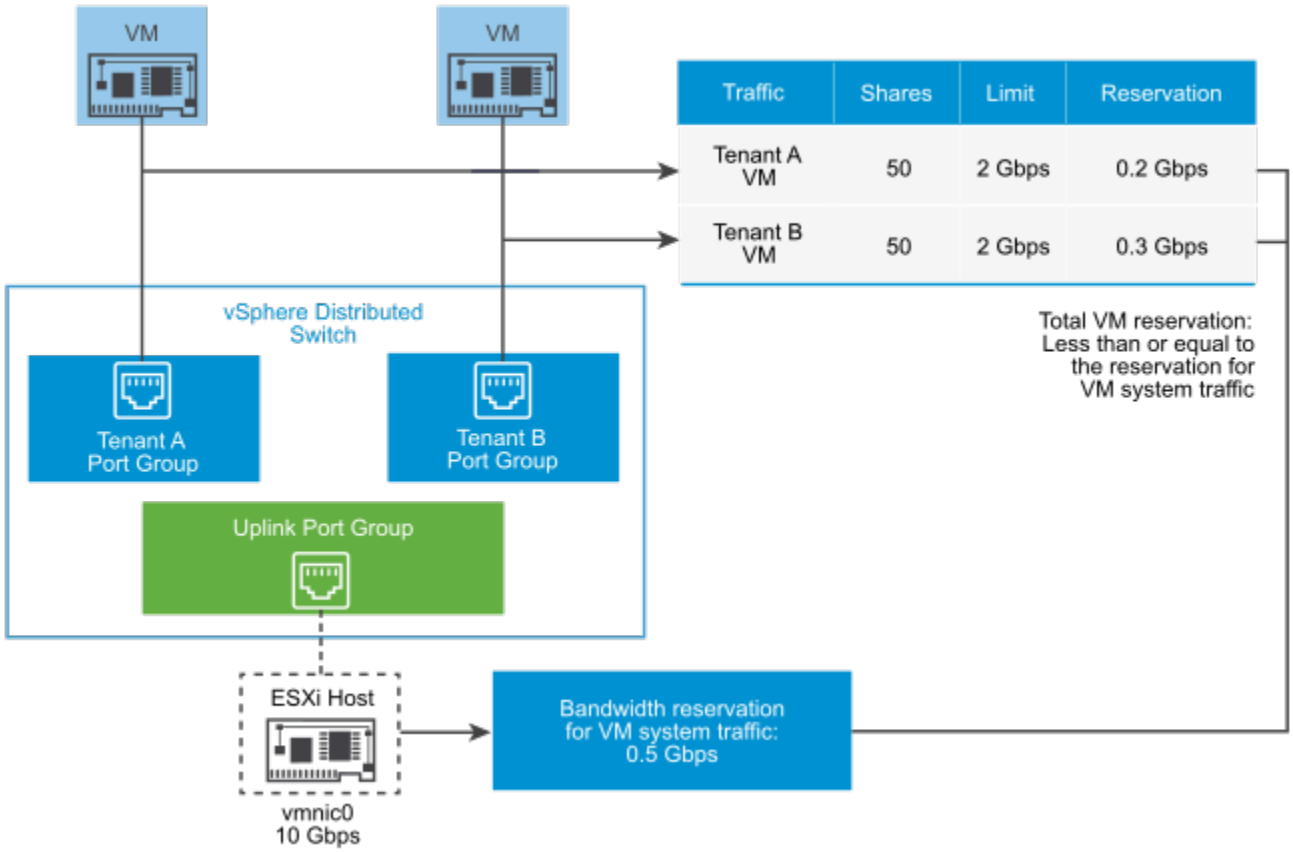
Bandwidth Provisioning to a Virtual Machine on the Host

To guarantee bandwidth, Network I/O Control implements a traffic placement engine that becomes active if a virtual machine has bandwidth reservation configured. The distributed switch attempts to place the traffic from a VM network adapter to the physical adapter that can supply the required bandwidth and is in the scope of the active teaming policy.

The total bandwidth reservation of the virtual machines on a host cannot exceed the reserved bandwidth that is configured for the virtual machine system traffic.

The actual limit and reservation also depends on the traffic shaping policy for the distributed port group the adapter is connected to. For example, if a VM network adapter requires a limit of 200 Mbps and the average bandwidth configured in the traffic shaping policy is 100 Mbps, then the effective limit becomes 100Mbps.

Figure 60: Configuration for Bandwidth Allocation for Individual Virtual Machines



The reservation of bandwidth for a VM in Network I/O Control is guaranteed against the reservation of VM system traffic on the physical adapter that sends the traffic from the VM.

Bandwidth Allocation Parameters for Virtual Machine Traffic

Network I/O Control version 3 allocates bandwidth to individual virtual machines based on configured shares, reservation, and limit for the network adapters in the VM hardware settings.

Table 192: Bandwidth Allocation Parameters for a VM Network Adapter

Parameter for Bandwidth Allocation	Description
Shares	The relative priority, from 1 to 100, of the traffic through this VM network adapter against the capacity of the physical adapter that is carrying the VM traffic to the network.
Reservation	The minimum bandwidth, in Mbps, that the VM network adapter must receive on the physical adapter.
Limit	The maximum bandwidth on the VM network adapter for traffic to other virtual machines on the same or on another host.

Admission Control for Virtual Machine Bandwidth

To guarantee that sufficient bandwidth is available to a virtual machine, vSphere implements admission control at host and cluster levels based on bandwidth reservation and teaming policy.

Bandwidth Admission Control in vSphere Distributed Switch

When you power on a virtual machine, the Network I/O Control feature on a distributed switch verifies that these conditions are satisfied on the host.

- A physical adapter on the host can supply the minimum bandwidth to the VM network adapters in accordance with the teaming policy and reservation.
- The reservation for a VM network adapter is less than the free quota in the network resource pool.

If you change the reservation for a network adapter of a running virtual machine, Network I/O Control verifies again whether the associated network resource pool can accommodate the new reservation. If the pool does not have enough unclaimed quota, the change is not applied.

To use admission control in vSphere Distributed Switch, perform the following tasks:

- Configure bandwidth allocation for the virtual machine system traffic on the distributed switch.
- Configure a network resource pool with a reservation quota from the bandwidth configured for virtual machine system traffic.
- Associate the network resource pool with the distributed port group that connects the virtual machines to the switch.
- Configure the bandwidth requirements of a virtual machine connected to the port group.

Bandwidth Admission Control in vSphere DRS

If you power on a virtual machine that is in a cluster, vSphere DRS places the virtual machine on a host that has the capacity to guarantee the bandwidth reserved for the virtual machine according to the active teaming policy.

vSphere DRS migrates a virtual machine to another host to satisfy the bandwidth reservation of the virtual machine in these situations:

- The reservation is changed to a value that the initial host can no longer satisfy.
- A physical adapter that carries traffic from the virtual machine is offline.

To use admission control in vSphere DRS, perform the following tasks:

- Configure bandwidth allocation for the virtual machine system traffic on the distributed switch.
- Configure the bandwidth requirements of a virtual machine that is connected to the distributed switch.

For more information about resource management according to bandwidth demands of virtual machines, see the *vSphere Resource Management* documentation.

Bandwidth Admission Control in vSphere HA

When a host fails or is isolated, vSphere HA powers on a virtual machine on another host in the cluster according to the bandwidth reservation and teaming policy.

To use admission control in vSphere HA, perform the following tasks:

- Allocate bandwidth for the virtual machine system traffic.
- Configure the bandwidth requirements of a virtual machine that is connected to the distributed switch.

For more information about vSphere HA provides failover based on the bandwidth demands of virtual machines, see the *vSphere Availability* documentation.

Create a Network Resource Pool

Create network resource pools on a vSphere Distributed Switch to reserve bandwidth for a set of virtual machines.

- Verify that vSphere Distributed Switch is version 6.5.0 and later.
- Verify that Network I/O Control on the switch is version 3.

A network resource pool provides a reservation quota to virtual machines. The quota represents a portion of the bandwidth that is reserved for virtual machine system traffic on the physical adapters connected to the distributed switch. You can set aside bandwidth from the quota for the virtual machines that are associated with the pool. The reservation from the network adapters of powered on VMs that are associated with the pool must not exceed the quota of the pool. See About Allocating Bandwidth for Virtual Machines.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Resource Allocation**.
3. Click **Network resource pools**.
4. Click the **Add** icon.
5. Optional: Type a name and a description for the network resource pool.
6. Enter a value for **Reservation quota**, in Mbps, from the free bandwidth that is reserved for the virtual machine system traffic.

   The maximum quota that you can assign to the pool is determined according to the following formula:

   ```
   max reservation quota = aggregated reservation for vm system traffic - quotas of the other resource pools
   ```

   where

   - `aggregated reservation for vm system traffic` = configured bandwidth reservation for the virtual machine system traffic on each pNIC * number of pNICs connected to the distributed switch
   - `quotas of the other pools` = the sum of the reservation quotas of the other network resource pools
7. Click **OK**.

Add one or more distributed port groups to the network resource pool so that you can allocate bandwidth to individual virtual machines from the quota of the pool. See Add a Distributed Port Group to a Network Resource Pool.

Add a Distributed Port Group to a Network Resource Pool

Add a distributed port group to a network resource pool so that you can allocate bandwidth to the virtual machines that are connected to the port group.

To assign a network resource pool to several distributed port groups at once, you can use the Resource allocation policy in the **Manage Distributed Port Groups** wizard. See Manage Policies for Multiple Port Groups on a vSphere Distributed Switch.

Network I/O Control allocates bandwidth to the virtual machines associated with the distributed port group according to the model implemented in the Network I/O Control version that is active on the distributed switch. See About vSphere Network I/O Control Version 3.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Right-click the distributed port group and select **Edit settings**.
3. In the Edit Settings dialog box, click **General**.
4. From the **Network resource pool** drop-down menu, select the network resource pool and click **OK**.

   If the distributed switch does not contain network resource pools, you see only the **(default)** option in the drop-down menu.

Configure Bandwidth Allocation for a Virtual Machine

You can configure bandwidth allocation to individual virtual machines that are connected to a distributed port group. You can use shares, reservation, and limit settings for bandwidth.

- Verify that vSphere Distributed Switch is version 6.5.0 and later.
- Verify that Network I/O Control on the switch is version 3.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. From the Actions menu, select Edit Settings.
3. Expand the Network adapter section of the VM network adapter.
4. If you want to configure bandwidth allocation for a new VM network adapter, from the **Add new device** drop-down menu select **Network adapter**.

   A New Network section displays options for bandwidth allocation and other network adapter settings.
5. If the VM network adapter is not connected to the distributed port group, select the port group from the drop-down menu next to the Network adapter or New Network label.
6. From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.

   Network I/O Control applies the configured shares when a physical adapter is saturated.

   You can select an option to set a pre-defined value, or select **Custom** and type a number from 1 to 100 to set another share.
7. In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.

   If you provision bandwidth by using a network resource pool, the reservation from the network adapters of powered on VMs that are associated with the pool must not exceed the quota of the pool.

   If vSphere DRS is enabled, to power on the virtual machine, make sure that the reservation from all VM network adapters on the host does not exceed the bandwidth reserved for virtual machine system traffic on the host physical adapters.

8. In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.
9. Click **OK**.

Network
I/O Control allocates the bandwidth that you reserved for the network adapter of the virtual machine out of the reservation quota of the network resource pool.

Configure Bandwidth Allocation on Multiple Virtual Machines

With a single operation, configure bandwidth allocation on multiple virtual machines that are connected to a specific network resource pool, for example, after you upgrade Network I/O Control to version 3.

- Verify that vSphere Distributed Switch is version 6.5.0 and later.
- Verify that Network I/O Control on the switch is version 3.
- Verify that the virtual machines are associated with a specific network resource pool through the connected distributed port groups. See Add a Distributed Port Group to a Network Resource Pool.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Resource Allocation**.
3. Click **Network resource pools**.
4. Select a network resource pool.
5. Click **Virtual Machines**.

   A list of the VM network adapters that are connected to the selected network resource pool appears.
6. Select the VM network adapters whose settings you want to configure and click **Edit**.
7. From the **Shares** drop-down menu, set the relative priority of traffic from these virtual machines in the scope of the physical adapters that carry the traffic.

   Network I/O Control applies the configured shares when a physical adapter is saturated.
8. In the **Reservation** text box, reserve a minimum bandwidth that must be available to each VM network adapter when the virtual machines are powered on.

   If you provision bandwidth by using a network resource pool, the reservation from the network adapters of powered on VMs that are associated with the pool must not exceed the quota of the pool.
9. In the **Limit** text box, set a limit on the bandwidth that each VM network adapter can consume.
10. Click **OK**.

Change the Quota of a Network Resource Pool

Change the quota of bandwidth that you can reserve for virtual machines connected to a set of distributed port groups.

- Verify that vSphere Distributed Switch is version 6.5.0 and later.

- Verify that Network I/O Control on the switch is version 3.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Resource Allocation**.
3. Click **Network resource pools**.
4. Select a network resource pool from the list and click **Edit**.
5. In the **Reservation quota** text box, enter the bandwidth quota for virtual machines from the aggregation of free bandwidth that is reserved for virtual machine system traffic on all physical adapters on the switch.
6. Click **OK**.

Remove a Distributed Port Group from a Network Resource Pool

To stop allocating bandwidth to the virtual machines from the reservation quota of a network resource pool, remove the association between the port group to which the virtual machines are connected and the pool.

1. Locate a distributed port group in the vSphere Client.
   a) Select a distributed switch and click the **Networks** tab.
   b) Click **Distributed Port Groups**.
2. Right-click the distributed port group and select **Edit Settings**.
3. In the Edit Settings dialog box for the port group, click **General**.
4. From the **Network resource pool** drop-down menu, select **(default)** and click **OK**.

The distributed port group becomes associated with the default VM network resource pool.

Delete a Network Resource Pool

Delete a network resource pool that is no longer in use.

Uncouple the network resource pool from all associated distributed port groups. See Remove a Distributed Port Group from a Network Resource Pool.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Resource Allocation**.
3. Click **Network resource pools**.
4. Select a network resource pool and click **Remove**.
5. Click **OK** to delete the resource pool.

Move a Physical Adapter Out the Scope of Network I/O Control

Under certain conditions you might need to exclude physical adapters with low capacity from the bandwidth allocation model of Network I/O Control version 3.

- Verify that the host is running ESXi 6.5 and later.

- Verify that vSphere Distributed Switch is version 6.5.0 and later.
- Verify that Network I/O Control on the switch is version 3.

For example, if the bandwidth allocation on a vSphere Distributed Switch is tailored on top of 10 GbE NICs, you might not be able to add a 1GbE NIC to the switch because it cannot meet the higher allocation requirements configured on the 10GbE NICs.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **System** and select **Advanced System Settings** .
3. Set the physical adapters that you need to function outside the scope of Network I/O Control as a comma-separated list to the `Net.IOControlPnicOptOut` parameter.
   For example: `vmnic0,vmnic3`
4. Click **OK** to apply the changes.

MAC Address Management

MAC addresses are used in the Layer 2 (Data Link Layer) of the network protocol stack to transmit frames to a recipient. In vSphere, vCenter Server generates MAC addresses for virtual machine adapters and VMkernel adapters, or you can assign addresses manually.

Each network adapter manufacturer is assigned a unique three-byte prefix called an Organizationally Unique Identifier (OUI), which it can use to generate unique MAC addresses.

VMware supports several address allocation mechanisms, each of them with a separate OUI:

- Generated MAC addresses
  - Assigned by vCenter Server
  - Assigned by the ESXi host
- Manually set MAC addresses
- Generated for legacy virtual machines, but no longer used with ESXi

If you reconfigure the network adapter of a powered off virtual machine, for example by changing the automatic MAC address allocation type, or setting a static MAC address, vCenter Server resolves any MAC address conflict before the adapter reconfiguration takes effect.

MAC Address Assignment from vCenter Server

vSphere provides several schemes for automatic allocation of MAC addresses in vCenter Server. You can select the scheme that best suits your requirements for MAC address duplication, OUI requirements for locally administered or universally administered addresses, and so on.

The following schemes of MAC address generation are available in vCenter Server:

- VMware OUI allocation, default allocation
- Prefix-based allocation
- Range-based allocation

After the MAC address is generated, it does not change unless the virtual machine's MAC address conflicts with that of another registered virtual machine. The MAC address is saved in the configuration file of the virtual machine.

Note: If you use invalid prefix- or range-based allocation values, an error is logged in the `vpxd.log` file. vCenter Server does not allocate MAC addresses when provisioning a virtual machine.

Preventing MAC Address Conflicts

The MAC address of a powered off virtual machine is not checked against the addresses of running or suspended virtual machines.

When a virtual machine is powered on again, it might acquire a different MAC address. The change might be caused by an address conflict with another virtual machine. While this virtual machine has been powered off, its MAC address has been assigned to another virtual machine that has been powered on.

If you reconfigure the network adapter of a powered off virtual machine, for example, by changing the automatic MAC address allocation type or setting a static MAC address, vCenter Server resolves MAC address conflicts before the adapter reconfiguration takes effect.

For information about resolving MAC address conflicts, see the *vSphere Troubleshooting* documentation.

VMware OUI Allocation

VMware Organizationally Unique Identifier (OUI) allocation assigns MAC addresses based on the default VMware OUI `00:50:56` and the vCenter Server ID.

VMware OUI allocation is the default MAC address assignment model for virtual machines. The allocation works with up to 64 vCenter Server instances, and each vCenter Server can assign up to 64000 unique MAC addresses. The VMware OUI allocation scheme is suitable for small scale deployments.

MAC Address Format

According to the VMware OUI allocation scheme, a MAC address has the format `00:50:56:`*`XX`*`:`*`YY`*`:`*`ZZ`* where `00:50:56` represents the VMware OUI, *`XX`* is calculated as (128+ vCenter Server ID), and *`YY`* and *`ZZ`* are random two-digit hexadecimal numbers.

The addresses created through the VMware OUI allocation are in the range `00:50:56:80:`*`YY`*`:`*`ZZ`* - `00:50:56:BF:`*`YY`*`:`*`ZZ`*.

Related Links

Duplicate MAC Addresses of Virtual Machines on the Same Network

Prefix-Based MAC Address Allocation

You can use prefix-based allocation to specify an OUI other than the default one `00:50:56` by VMware, or to introduce Locally Administered MAC Addresses (LAA) for a larger address space.

Prefix-based MAC address allocation overcomes the limits of the default VMware allocation to provide unique addresses in larger scale deployments. Introducing an LAA prefix leads to a very large MAC address space (2 to the power of 46) instead of an universally unique address OUI which can give only 16 million MAC addresses.

Verify that the prefixes that you provide for different vCenter Server instances in the same network are unique. vCenter Server relies on the prefixes to avoid MAC address duplication issues, see Troubleshooting MAC Address Allocation.

Note: Prefix-based MAC address allocation settings are lost when you upgrade to a new version of vCenter Server. You must manually recreate the prefix-based MAC address allocation settings after the upgrade.

Related Links

Duplicate MAC Addresses of Virtual Machines on the Same Network

Range-Based MAC Address Allocation

You can use range-based allocation to include or exclude ranges of Locally Administered Addresses (LAA).

You specify one or more ranges using a starting and ending MAC addresses, for example, (`02:50:68:00:00:02` , `02:50:68:00:00:FF`). MAC addresses are generated only from within the specified range.

You can specify multiple ranges of LAA, and vCenter Server tracks the number of used addresses for each range. vCenter Server allocates MAC addresses from the first range that still has addresses available. vCenter Server checks for MAC address conflicts within its ranges.

When using range-based allocation, you must provide different instances of vCenter Server with ranges that do not overlap. vCenter Server does not detect ranges that might be in conflict with other vCenter Server instances. See the Troubleshooting MAC Address Allocation for more information about resolving issues with duplicate MAC addresses.

Note: Range-based MAC address allocation settings are lost when you upgrade to a new version of vCenter Server. You must manually recreate the range-based MAC address allocation settings after the upgrade.

Related Links

Duplicate MAC Addresses of Virtual Machines on the Same Network

Assigning a MAC Address

Use the vSphere Client to enable prefix-based or range-based MAC address allocation and to adjust the allocation parameters.

If you are changing from one type of allocation to another, for example changing from the VMware OUI allocation to a range-based allocation, use the vSphere Client. However, when a schema is prefix-based or range-based and you want to change to a different allocation schema, you must edit the `vpxd.cfg` file manually and restart vCenter Server.

Change to or Adjust Range- or Prefixed-Based Allocations

By switching from the default VMware OUI to range- or prefixed-based MAC address allocation through the vSphere Client, you can avoid and resolve MAC address duplication conflicts in vSphere deployments.

Change the allocation scheme from the default VMware OUI to range- or to prefixed-based allocation by using the **Advanced Settings** available for the vCenter Server instance in the vSphere Client.

To switch from range- or prefixed-based allocation back to VMware OUI allocation, or between range- and prefixed-based allocation, edit the `vpxd.cfg` file manually. See Set or Change Allocation Type.

1. In the vSphere Client, navigate to a vCenter Server instance.
2. On the **Configure** tab, expand **Settings** and select **Advanced Settings**.
3. Click **Edit Settings.**
4. Add or edit parameters for the target allocation type.
   Use only one allocation type.
   - Change to prefix-based allocation.

Key	Example Value
`config.vpxd.macAllocScheme.prefixScheme.prefix`	005026

Key	Example Value
config.vpxd.macAllocScheme.prefixScheme.prefixLength	23

`prefix` and `prefixLength` determine the range of MAC address prefixes that newly added vNICs have. `prefix` is the starting OUI of MAC addresses related to the instance, and `prefixLength` determines the length of the prefix in bits.

For example, the settings from the table result in VM NIC MAC addresses starting with 00:50:26 or 00:50:27.

- Change to range-based allocation.

Key	Example Value
config.vpxd.macAllocScheme.rangeScheme.range[X].begin	005067000000
config.vpxd.macAllocScheme.rangeScheme.range[X].end	005067ffffff

X in `range[X]` stands for the range sequence number. For example, `0` in `range[0]` represents the allocation settings of the first range for MAC address allocation.

5. Click **Save**.

Set or Change Allocation Type

If you are changing from range- or prefixed-based allocation to the VMware OUI allocation, you must set the allocation type in the `vpxd.cfg` file and restart the vCenter Server.

Decide on an allocation type before changing the `vpxd.cfg` file. For information on allocation types, see MAC Address Assignment from vCenter Server

1. On the host machine of , navigate to the directory `/etc/vmware-vpx`.
2. Open the `vpxd.cfg` file.
3. Decide on an allocation type to use and enter the corresponding XML code in the file to configure the allocation type.
   The following are examples of XML code to use.

   Note: Use only one allocation type.

   - VMware OUI allocation

     ```
     <vpxd>
        <macAllocScheme>
           <VMwareOUI>true</VMwareOUI>
        </macAllocScheme>
     </vpxd>
     ```

   - Prefix-based allocation

     ```
      <vpxd>
         <macAllocScheme>
           <prefixScheme>
              <prefix>005026</prefix>
              <prefixLength>23</prefixLength>
           </prefixScheme>
        </macAllocScheme>
     ```

```
</vpxd>
```

- Range-based allocation

```
<vpxd>
   <macAllocScheme>
       <rangeScheme>
          <range id="0">
             <begin>005067000001</begin>
             <end>005067000001</end>
          </range>
       </rangeScheme>
   </macAllocScheme>
</vpxd>
```

4. Save the `vpxd.cfg` .
5. Restart the vCenter Server host.

MAC Address Generation on ESXi Hosts

An ESXi host generates the MAC address for a virtual machine adapter when the host is not connected to vCenter Server. Such addresses have a separate VMware OUI to avoid conflicts.

The ESXi host generates the MAC address for a virtual machine adapter in one of the following cases:

- The host is not connected to vCenter Server.
- The virtual machine configuration file does not contain the MAC address and information about the MAC address allocation type.

MAC Address Format

The host generates MAC addresses that consists of the VMware OUI `00:0C:29` and the last three octets in hexadecimal format of the virtual machine UUID. The virtual machine UUID is based on a hash calculated by using the UUID of the ESXi physical machine and the path to the configuration file (`.vmx`) of the virtual machine.

Preventing MAC Address Conflicts

All MAC addresses that have been assigned to network adapters of running and suspended virtual machines on a given physical machine are tracked for conflicts.

If you import a virtual machine with a host-generated MAC address from one vCenter Server to another, select the **I Copied It** option when you power on the virtual machine to regenerate the address and avoid potential conflicts in the target vCenter Server or between the vCenter Server systems.

Setting a Static MAC Address to a Virtual Machine

In most network deployments, generated MAC addresses are a good approach. However, you might need to set a static MAC address for a virtual machine adapter with unique value.

The following cases show when you might set a static MAC address:

- Virtual machine adapters on different physical hosts share the same subnet and are assigned the same MAC address, causing a conflict.
- Ensure that a virtual machine adapter always has the same MAC address.

By default, VMware uses the Organizationally Unique Identifier (OUI) `00:50:56` for manually generated addresses, but all unique manually generated addresses are supported.

Note: Make sure that no other non-VMware devices use addresses assigned to VMware components. For example, you might have physical servers in the same subnet, which use `11:11:11:11:11:11` , `22:22:22:22:22:22` as static MAC addresses. The physical servers do not belong to the vCenter Server inventory, and vCenter Server is not able to check for address collision.

VMware OUI in Static MAC Addresses

By default, static MAC addresses have the VMware Organizationally Unique Identifier (OUI) as the prefix. However, the range of free address provided by the VMware OUI is restricted.

If you decide to use the VMware OUI, part of the range is reserved for use by vCenter Server, host physical NICs, virtual NICs, and for future use.

You can set a static MAC address that contains the VMware OUI prefix in compliance with the following format:

`00:50:56:XX:YY:ZZ`

where *XX* is a valid hexadecimal number between 00 and 3F, and *YY* and *ZZ* are valid hexadecimal numbers between 00 and FF. To avoid conflict with MAC addresses that are generated by vCenter Server or are assigned to VMkernel adapters for infrastructure traffic, the value for *XX* must not be greater than 3F.

The maximum value for a manually generated MAC address is as follows.

`00:50:56:3F:FF:FF`

To avoid conflicts between the generated MAC addresses and the manually assigned ones, select a unique value for *XX*:*YY*:*ZZ* from your hard-coded addresses.

Assign a Static MAC Address

You can assign static MAC addresses to the virtual NIC of a powered off virtual machine by using the vSphere Client.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. Power off the virtual machine.
3. From the Actions menu, select Edit Settings.
4. Select the **Virtual Hardware** tab in the dialog box displaying the settings.
5. Expand the network adapter section.
6. Under MAC Address, select **Manual** from the drop-down menu.
7. Type the static MAC address, and click **OK**.
8. Power on the virtual machine.

Related Links

Duplicate MAC Addresses of Virtual Machines on the Same Network

Assign a Static MAC Address in the Virtual Machine Configuration File

To set a static MAC address for a virtual machine, you can edit the configuration file of the virtual machine by using the vSphere Client.

1. Locate the virtual machine in the .
   a) Select a data center, folder, cluster, resource pool, or host and click the **VMs** tab.
   b) Click **Virtual Machines** and click the virtual machine from the list.
2. Power off the virtual machine.
3. From the **Actions** drop-down menu, select **Edit Settings**.
4. Select the **VM Options** tab and expand **Advanced**.
5. Click **Edit Configuration**.
6. To assign a static MAC address, add or edit parameters as required.

Parameter	Value
`ethernet`*`X`*`.addressType`	`static`
`ethernet`*`X`*`.address`	*`MAC_address_of_the_virtual_NIC`*

   `X` next to `ethernet` stands for the sequence number of the virtual NIC in the virtual machine.

   For example, `0` in `ethernet0` represents the settings of the first virtual NIC device added to the virtual machine.
7. Click **OK**.
8. Power on the virtual machine.

Configuring vSphere for IPv6

Configure ESXi hosts and vCenter Server for operation in a pure IPv6 environment for larger address space and improved address assignment.

IPv6 is designated by the Internet Engineering Task Force (IETF) as the successor to IPv4 providing the following benefits:

- Increased address length. The increased address space resolves the problem of address exhaustion and eliminates the need for network address translation. IPv6 uses 128-bit addresses compared with the 32-bit addresses used by IPv4.
- Ability for improved address autoconfiguration of nodes.

vSphere IPv6 Connectivity

In an environment that is based on vSphere 6.0 and later, nodes and features can communicate over IPv6 transparently supporting static and automatic address configuration.

IPv6 in the Communication between vSphere Nodes

The nodes in a vSphere deployment can communicate using IPv6 and accept assigned addresses according to the network configuration.

Table 193: IPv6 Support of the Nodes in a vSphere Environment

Connection Type	IPv6 Support	Address Configuration of vSphere nodes
ESXi to ESXi	Yes	• Static • Automatic: AUTOCONF/DHCPv6
vCenter Server machine to ESXi	Yes	• Static • Automatic: AUTOCONF/DHCPv6
vCenter Server machine to machine	Yes	• Static • Automatic: AUTOCONF/DHCPv6
ESXi to vSphere Client machine	Yes	• Static • Automatic: AUTOCONF/DHCPv6
Virtual machine to virtual machine	Yes	• Static • Automatic: AUTOCONF/DHCPv6
ESXi to iSCSI Storage	Yes	• Static • Automatic: AUTOCONF/DHCPv6
ESXi to NFS Storage	Yes	• Static • Automatic: AUTOCONF/DHCPv6
ESXi to Active Directory	No Use LDAP through vCenter Server to connect ESXi to the Active Directory database	-
vCenter Server to Active Directory	No Use LDAP to connect vCenter Server to the Active Directory database	-

IPv6 Connectivity of vSphere Features

Certain vSphere features do not support IPv6:

- vSphere DPM over Intelligent Platform Management Interface (IPMI) and Hewlett-Packard Integrated Lights-Out (iLO). vSphere 6.5 and later supports only Wake-On-LAN (WOL) to bring a host out of standby mode.
- Authentication Proxy
- vSphere Management Assistant and ESXCLI connected to Active Directory.
  Use LDAP to connect the vSphere Management Assistant or the ESXCLI to the Active Directory database.

IPv6 Connectivity of Virtual Machines

Virtual machines can exchange data in the network over IPv6. vSphere supports both static and automatic assignment of IPv6 addresses for virtual machines.

Configuring one or more IPv6 addresses is also possible when you customize the guest operating system of a virtual machine.

vSAN Connectivity

vSAN supports IPv6. Use NFS 4.1 with AUTH_SYS.

FQDNs and IPv6 Addresses

In vSphere, you should use fully qualified domain names (FQDNs) that are mapped to IPv6 addresses on the DNS server. You can use IPv6 addresses if they have a valid FQDN on the DNS server for reverse lookup.

To deploy vCenter Server in a pure IPv6 environment, you must use FQDNs only.

Deploying vSphere on IPv6

Run vSphere in a pure IPv6 environment to use an extended address space and flexible address assignment.

If you plan to deploy vCenter Server and ESXi hosts in an IPv6 network, you must perform additional steps.

Enable IPv6 on a vSphere Installation

If you have a greenfield deployment of vSphere 6.5 in an IPv6 network, configure ESXi and vCenter Server for pure IPv6 management connection by configuring IPv6 on the deployment nodes and connecting them.

- Verify that the IPv6 addresses for vCenter Server, the ESXi hosts and an external database, if used, are mapped to fully qualified domain names (FQDNs) on the DNS server.
- Verify that the network infrastructure provides IPv6 connectivity for the ESXi hosts, vCenter Server and external database if used.
- Verify that you have version 6.5 of vCenter Server installed with FQDN that is mapped to an IPv6 address. See the *vCenter Server Installation and Setup* documentation.
- Verify that the hosts have ESXi 6.5 installed. See the *vCenter Server Installation and Setup* documentation.

1. In the Direct Console User Interface (DCUI), configure each ESXi host as a pure IPv6 node.
   a) In the DCUI, press F2 and log in to the host.
   b) From the **Configure Management Network** menu, select **IPv6 Configuration** and press Enter.
   c) Assign an IPv6 address to the host.

Address Assignment Option	Description
Automatic address assignment using DHCPv6	1. Select the **Use dynamic IPv6 address and network configuration** option and select **Use DHCPv6**. 2. Press Enter to save the changes.
Static address assignment	1. Select the **Set static IPv6 address and network configuration** option and enter the IPv6 address of the host and the default gateway. 2. Press Enter to save the changes.

   d) From the **Configure Management Network** menu, select **IPv4 Configuration** and press Enter.
   e) Select **Disable IPv4 configuration for management network** and press Enter.

2. In the vSphere Client, add the hosts to the inventory.

Related Links

Enable IPv6 on an Upgraded vSphere Environment on page 2331

On an IPv4 deployment of vSphere 6.5 that consists of an installed or upgraded vCenter Server and upgraded ESXi, configure ESXi and vCenter Server for pure IPv6 management connection by enabling IPv6 on the deployed nodes and reconnecting them.

Set Up IPv6 on vCenter Server on page 2333

Use the vSphere Client to configure vCenter Server for communication with ESXi hosts in an IPv6 network.

Set Up vCenter Server on Windows with IPv6

Enable IPv6 on an Upgraded vSphere Environment

On an IPv4 deployment of vSphere 6.5 that consists of an installed or upgraded vCenter Server and upgraded ESXi, configure ESXi and vCenter Server for pure IPv6 management connection by enabling IPv6 on the deployed nodes and reconnecting them.

- Verify that the network infrastructure provides IPv6 connectivity for the ESXi hosts, vCenter Server and external database if used.
- Verify that the IPv6 addresses for vCenter Server, the ESXi hosts and an external database, if used, are mapped to fully qualified domain names (FQDNs) on the DNS server.
- Verify that you have version 6.x of vCenter Server installed or upgraded. See the *vCenter Server Installation and Setup* and *vCenter Server Upgrade* documentation.
- Verify that all ESXi hosts are upgraded to version 6.x. See the *VMware ESXi Upgrade* documentation.

1. In the vSphere Client, disconnect the hosts from vCenter Server.
2. Configure each ESXi host as a pure IPv6 node.
   a) Open an SSH connection and log in to the ESXi host.
   b) Run the following command:
      ```
      esxcli network ip interface ipv6 set -i vmk0 -e true
      ```
   c) Assign an IPv6 address to the management network.

Address Assignment Option	Description

Static address assignment	1. Open an SSH connection and log in to the ESXi host.
	2. Set a static IPv6 address for the management network vmk0 by running the following command:
	`esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0`
	3. Set the default gateway for the management network vmk0 by running the following command:
	`esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address`
	4. Add a DNS server by running the following command:
	`esxcli network ip dns server add -s DNS_server_IPv6_address`

Automatic address assignment using DHCPv6	1. Open an SSH connection and log in to the ESXi host.
	2. Enable DHCPv6 for the management network vmk0 by running the following command:
	`esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true`
	3. Enable IPv6 Router Advertised for the management network vmk0 by running the following command:
	`esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true`
	4. Add a DNS server or use the DNS setting published by DHCPv6 by running one the following commands:
	`esxcli network ip dns server add -s DNS_server_IPv6_address`
	`esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true`

3. Deactivate the IPv4 configuration for the management network.
   a) Open an SSH connection and log in to the ESXi host.
   b) Run the following command:
   ```
   esxcli network ip interface ipv4 set -i vmk0 --type=none
   ```
4. If vCenter Server uses an external database, configure the database as an IPv6 node.
5. Configure vCenter Server as a pure IPv6 node and restart it.
6. Deactivate the IPv4 on the database server.
7. In the vSphere Client, add the hosts to the inventory.
8. Deactivate the IPv4 in the network infrastructure.

Related Links

Enable IPv6 on a vSphere Installation on page 2330

If you have a greenfield deployment of vSphere 6.5 in an IPv6 network, configure ESXi and vCenter Server for pure IPv6 management connection by configuring IPv6 on the deployment nodes and connecting them.

Set Up IPv6 on vCenter Server on page 2333

Use the vSphere Client to configure vCenter Server for communication with ESXi hosts in an IPv6 network.

Set Up vCenter Server on Windows with IPv6

Activate or Deactivate IPv6 Support on a Host

The IPv6 support in vSphere lets hosts work in an IPv6 network that has a large address space, enhanced multicasting, simplified routing, and so on.

In ESXi 6.0 and later releases, IPv6 is enabled by default.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **TCP/IP Configuration**.
3. Click **Edit**.
4. Use the toggle button to activate or deactivate IPv6 support.
5. Click **OK**.
6. Reboot the host to apply the changes in the IPv6 support.

Configure the IPv6 settings of VMkernel adapters on the host, for example, of the management network. See Set Up IPv6 on an ESXi Host.

Set Up IPv6 on an ESXi Host

To connect an ESXi host over IPv6 to the management network, vSphere vMotion, shared storage, vSphere Fault Tolerance, and so on, edit the IPv6 settings of the VMkernel adapters on the host.

Verify that IPv6 is enabled on the ESXi host. See Activate or Deactivate IPv6 Support on a Host .

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **VMkernel adapters**.
3. Select the VMkernel adapter on the target distributed or standard switch and click **Edit**.
4. In the Edit Settings dialog box, click **IPv6 settings**.
5. Configure the address assignment of the VMkernel adapter.

IPv6 Address Option	Description
Obtain IPv6 address automatically through DHCP	Receive an IPv6 address for the VMkernel adapter from a DHCPv6 server.
Obtain IPv6 address automatically through Router Advertisement	Receive an IPv6 address for the VMkernel adapter from a router through Router Advertisement.
Static IPv6 addresses	Set one or more addresses. For each address entry, enter the IPv6 address of the adapter, subnet prefix length and IPv6 address of the default gateway.

   You can select several assignment options according the configuration of your network.

6. Click **OK** to apply the changes on the VMkernel adapter.

Related Links

Create a VMkernel Adapter on a vSphere Standard Switch on page 2195

Create a VMkernel network adapter on a vSphere standard switch to provide network connectivity for hosts and to handle the system traffic for vSphere vMotion, IP storage, Fault Tolerance logging, vSAN, and so on. You can also create VMkernel adapters on the source and target vSphere Replication hosts to isolate the replication data traffic. Dedicate a VMkernel adapter to only one traffic type.

Create a VMkernel Adapter on a Host Associated with a vSphere Distributed Switch on page 2208

Create a VMkernel adapter on a host that is associated with a distributed switch to provide network connectivity to the host and to handle the traffic for vSphere vMotion, IP storage, Fault Tolerance logging, vSAN, and others. You can set up VMkernel adapters for the standard system traffic on vSphere standard switches and on vSphere distributed switches.

Set Up IPv6 on vCenter Server

Use the vSphere Client to configure vCenter Server for communication with ESXi hosts in an IPv6 network.

1. On the vSphere Client main page, click **Administration** > **Deployment** > **System Configuration**.
2. Under **System Configuration**, select a node from the list.
3. Click **Login**.
4. Use the vSphere Client to log in as administrator@*`your_domain_name`* to the vCenter Server instance.
   The address is of the type http://*`appliance-IP-address-or-FQDN`*/ui.

5. Under Common, select **Networking** and click **Edit**.
6. Expand the network interface name to edit the IP address settings.
7. Edit the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically through DHCP	Assigns IPv6 addresses to the appliance automatically from the network by using DHCP.
Obtain IPv6 settings automatically through router advertisement	Assigns IPv6 addresses to the appliance automatically from the network by using router advertisement.
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1. Click the checkbox. 2. Enter the IPv6 address and the subnet prefix length. 3. Click **Add** to enter additional IPv6 addresses. 4. Click **Save**.

   You can configure the appliance to obtain the IPv6 settings automatically through both DHCP and router advertisement. You can assign static a IPv6 address at the same time.

8. Optional: To remove IPv6 addresses that are assigned automatically through Router Advertisement, click **Remove Addresses** and delete the addresses.

   You might want to delete certain IPv6 addresses that vCenter Server obtained through Router Advertisement to stop the communication on these addresses and to enforce the configured static addresses.

Connect the ESXi hosts to vCenter Server over IPv6 by using their FQDNs.

Monitoring Network Connection and Traffic

Monitor network connection and packets that pass through the ports of a vSphere Standard Switch or a vSphere Distributed Switch to analyze the traffic between virtual machines and hosts.

Capture Network Packets by Using the PacketCapture Utility

Use the PacketCapture utility to diagnose networking problems such as slow connection, lost packets, and connectivity problems

PacketCapture is a lightweight tcpdump utility that captures and stores only the minimum amount of data that is needed to diagnose the network problem. PacketCapture is integrated in the rhttpproxy service of ESXi and vCenter Server. You start and stop PacketCapture by editing the rhttpproxy service XML configuration file.

1. Start capturing packets.
   a) Open an SSH connection and log in to the ESXi host or vCenter Server.
   b) Open the `config.xml` file for editing.

vSphere Component	File Location
ESXi	`/etc/vmware/rhttpproxy/config.xml`
vCenter Server	`/etc/vmware-rhttpproxy/config.xml`

   c) Make the following changes.

```
<config>
  <packetCapture>
    <enabled>true</enabled>
```

d) Optional: Configure PacketCapture options.

Option and Default Value	Description
<validity>72</validity>	On startup delete all `pcap` and `pcap.gz` files that were last modified before the specified period of hours and are not part of the current process.
<directory>/directory_path</directory>	The directory in which `pcap` and `pcap.gz` files are stored. The directory must exist and be accessible.
<maxDataInPcapFile>52428800</maxDataInPcapFile>	The amount of captured data in bytes that each `pcap` and `pcap.gz` file can store before rolling over to the next file. The minimum size is 5 MB on vCenter Server and 2.5MB on ESXi. **Note:** Storing 50 MB of captured data in a `pcap` file requires a `pcap` file of about 67.5 MB.
<maxPcapFilesCount>5</maxPcapFilesCount>	The number of `pcap` or `pcap.gz` files to rotate. The minimum number is 2.

e) Save and close the `config.xml` file.

f) Reload the `config.xml` file by running the following command.

```
kill -SIGHUP `pidof rhttpproxy`
```

2. Stop capturing packets.

a) Open an SSH connection and log in to the ESXi host or vCenter Server.

b) Open the `config.xml` file for editing.

c) Make the following changes.

```
<config>
  <packetCapture>
    <enabled>false</enabled>
```

d) Save and close the `config.xml` file.

e) Reload the `config.xml` file by running the following command.

```
kill -SIGHUP `pidof rhttpproxy`
```

3. Collect the captured data.

The `pcap` or `pcap.gz` files are stored in the following default directories.

vSphere Component	File Location
ESXi	`/var/run/log`
vCenter Server	`/var/log/vmware/rhttpproxy`

Copy the `pcap` and `pcap.gz` files to a system that runs a network analyzer tool, such as Wireshark, and examine the packet details.

Before you analyze the `pcap` and `pcap.gz` captured from an ESXi host, use the TraceWrangler utility to fix the frame size metadata. For more information, see https://kb.vmware.com/kb/52843

Capturing and Tracing Network Packets by Using the pktcap-uw Utility

Monitor the traffic that flows through physical network adapters, VMkernel adapters, and virtual machines adapters, and analyze packet information by using the graphical user interface of network analysis tools such as Wireshark.

In vSphere you can monitor packets on a host by using the `pktcap-uw` console utility. You can use the utility without additional installation on an ESXi host. `pktcap-uw` provides many points in the host network stack at which you can monitor traffic.

For detailed analysis of captured packets, you can save packet content from the `pktcap-uw` utility to files in PCAP or PCAPNG format and open them in Wireshark. You can also troubleshoot dropped packets and trace a packet's path in the network stack.

Note: The `pktcap-uw` utility is not fully supported for backward compatibility across vSphere releases. The options of the utility might change in the future.

pktcap-uw Command Syntax for Capturing Packets

Use the `pktcap-uw` utility to inspect the contents of packets while they traverse the network stack on an ESXi host.

pktcap-uw Syntax for Capturing Packets

The `pktcap-uw` command has the following syntax for capturing packets at a certain place in the network stack:

```
pktcap-uwswitch_port_argumentscapture_point_optionsfilter_optionsoutput_control_options
```

Note: Certain options of the `pktcap-uw` utility are designed for VMware internal use only and you should use them only under the supervision of VMware Technical Support. These options are not described in the *vSphere Networking* guide.

Table 194: pktcap-uw Arguments for Capturing Packets

Argument Group	Argument	Description
switch_port_arguments	`--uplink vmnic`*X*	Capture packets that are related to a physical adapter. You can combine the --uplink and --capture options for monitoring packets at a certain place in the path between the physical adapter and the virtual switch. See Capture Packets That Arrive at a Physical Adapter.
	`--vmk vmk`*X*	Capture packets that are related to a VMKernel adapter. You can combine the vmk and --capture options for monitoring packets at a certain place in the path between the VMkernel adapter and the virtual switch. See Capture Packets for a VMkernel Adapter.
	`--switchport {`*vmxnet3_port_ID* `|` *vmkernel_adapter_port_ID*`}`	Capture packets that are related to a VMXNET3 virtual machine adapter or to a VMkernel adapter that is connected to a particular virtual switch port. You can view the ID of the port in the network panel of the `esxtop` utility. You can combine the switchport and capture options for monitoring packets at a certain place in the path between the VMXNET3 adapter or VMkernel adapter and the virtual switch.

Argument Group	Argument	Description
		See Capture Packets for a VMXNET3 Virtual Machine Adapter.
	`--lifID`*`lif_ID`*	Capture packets that are related to the logical interface of a distributed router. See the *VMware NSX* documentation.
`capture_point_options`	`--capture`*`capture_point`*	Capture packets at a particular place in the network stack. For example, you can monitor packets right after they arrive from a physical adapter.
	--dir {0|1|2}	Capture packets according to the direction of the flow with regard to the virtual switch. 0 stands for incoming traffic, 1 for outgoing traffic, and 2 for bidirectional traffic. By default, the `pktcap-uw` utility captures ingress traffic. Use the --dir option together with the --uplink, --vmk, or --switchport option.
	--stage {0|1}	Capture the packet closer to its source or to its destination. Use this option to examine how a package changes while it traverses the points in the stack. 0 stands for traffic closer to source and 1 for traffic closer to destination. Use the --stage option together with the --uplink, --vmk , --switchport, or --dvfilter option.
	`--dvfilter`*`filter_name`* `--capture PreDVFilter|PostDVFilter`	Capture packets before or after a vSphere Network Appliance (DVFilter) intercepts them. See Capture Packets at DVFilter Level.
	-A | --availpoints	View all capture points that the `pktcap-uw` utility supports.
	For details about the capture points of the `pktcap-uw` utility, see Capture Points of the pktcap-uw Utility.	
`filter_options`	Filter captured packets according to source or destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port. See pktcap-uw Options for Filtering Packets.	
`output_control_options`	Save the contents of a packet to a file, capture only a number of packets, and capture a number of bytes at the beginning of packets, and so on. See pktcap-uw Options for Output Control.	

The vertical bars | represent alternative values, and the curly brackets {} used with vertical bars specify a list of choices for an argument or option.

pktcap-uw Command Syntax for Tracing Packets

Use the `pktcap-uw` utility to view the path of a packet in the network stack on an ESXi host for latency analysis.

pktcap-uw Syntax for Tracing Packets

The command of the `pktcap-uw` utility has the following syntax for tracing packets in the network stack:

```
pktcap-uw --trace filter_optionsoutput_control_options
```

Options to the pktcap-uw Utility for Tracing Packets

The `pktcap-uw` utility supports the following options when you use it to trace packets:

Table 195: pktcap-uw Options for Tracing Packets

Argument	Description
filter_options	Filter traced packets according to source or destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port. See pktcap-uw Options for Filtering Packets.
output_control_options	Save the contents of a packet to a file and trace only a number of packets. See pktcap-uw Options for Output Control.

Related Links

Trace Packets by Using the pktcap-uw Utility on page 2349

Use the `pktcap-uw` utility to trace the path that packets traverse in the network stack for latency analysis and for locating the point where a packet is corrupted or dropped.

pktcap-uw Options for Output Control

Use the options for output control of the `pktcap-uw` utility to save packet contents to a file, capture up to a certain number of bytes from each packet, and limit the number of captured packets.

pktcap-uw Options for Output Control

The options of the `pktcap-uw` utility for output control are valid when you capture and trace packets. For information about the command syntax of the `pktcap-uw` utility, see pktcap-uw Command Syntax for Capturing Packets and pktcap-uw Command Syntax for Tracing Packets.

Table 196: Options for Output Control That Are Supported by the pktcap-uw Utility

Option	Description
{-o | --outfile} *pcap_file*	Save captured or traced packets to a file in packet capture (PCAP) format. Use this option to examine packets in a visual analyzer tool such as Wireshark.
-P | --ng	Save packet content in the PCAPNG file format. Use this option together with the -o or --outfile option.
--console	Print packet details and content to the console output. By default, the `pktcap-uw` utility shows packet information in the console output.
{-c | --count} *number_of_packets*	Capture the first *number_of_packets* packets.
{-s | --snaplen} *snapshot_length*	Capture only the first *snapshot_length* bytes from each packet. If traffic on the host is intensive, use this option to reduce the load on the CPU and storage.

Option	Description
	To limit the size of captured contents, set a value greater than 24. To capture the complete packet, set this option to 0.
`-h`	View help about the `pktcap-uw` utility.

The vertical bars | represent alternative values, and the curly brackets {} used with vertical bars specify a list of choices for an argument or option.

pktcap-uw Options for Filtering Packets

Narrow the range of packets that you monitor by using the `pktcap-uw` utility to apply filtering options for source and destination address, VLAN, VXLAN, and next level protocol consuming the packet payload.

Filter Options

The filter options for `pktcap-uw` are valid when you capture and trace packets. For information about the command syntax of the `pktcap-uw` utility, see pktcap-uw Command Syntax for Capturing Packets and pktcap-uw Command Syntax for Tracing Packets.

Table 197: Filter Options of the pktcap-uw Utility

Option	Description
`--srcmac` *`mac_address`*	Capture or trace packets that have a specific source MAC address. Use colons to separate the octets in it.
`--dstmac` *`mac_address`*	Capture or trace packets that have a specific destination MAC address. Use colons to separate the octets in it.
`--mac` *`mac_address`*	Capture or trace packets that have a specific source or destination MAC address. Use colons to separate the octets in it.
`--ethtype 0x`*`Ethertype`*	Capture or trace packets at Layer 2 according to the next level protocol that consumes the packet payload. *`EtherType`* corresponds to the EtherType field in Ethernet frames. It represents the type of next level protocol that consumes the payload of the frame. For example, to monitor traffic for the Link Layer Discovery Protocol (LLDP) protocol, type `--ethtype 0x88CC`.
`--vlan` *`VLAN_ID`*	Capture or trace packets that belong to a VLAN.
`--srcip` *`IP_addess|IP_address/subnet_range`*	Capture or trace packets that have a specific source IPv4 address or subnet.
`--dstip` *`IP_addess|IP_address/subnet_range`*	Capture or trace packets that have a specific destination IPv4 address or subnet.
`--ip` *`IP_addess`*	Capture or trace packets that have a specific source or destination IPv4 address.
`--proto 0x`*`IP_protocol_number`*	Capture or trace packets at Layer 3 according to the next level protocol that consumes the payload. For example, to monitor traffic for the UDP protocol, type `--proto 0x11`.
`--srcport` *`source_port`*	Capture or trace packets according to their source TCP port.
`--dstport` *`destination_port`*	Capture or trace packets according to their destination TCP port.

Option	Description
`--tcpport` *`TCP_port`*	Capture or trace packets according to their source or destination TCP port.
`--vxlan` *`VXLAN_ID`*	Capture or trace packets that belong to a VXLAN.
`--rcf` *`pcap_filter_expression`*	Capture or trace packets using the rich common filter expression. For example, to capture all ingress and egress packets whose IP content length is larger than 1000 bytes, use the filter expression `--rcf "ip[2:2]>1000"`. To select a specific source host address and port number, use the filter expression `--rcf "src host 12.0.0.1 and port 5000"`. This example filters traffic for the host address 12.0.0.1 using port 5000. To learn more about filtering network traffic with the `--rcf` option, refer to the documentation for pcap filter expressions using command-line packet analyzers such as `tcpdump`. See pcap-filter - packet filter syntax. **Note:** When using the `--rcf` option, obey the following limitations. • Do not filter VLAN packets using the `--rcf` option. To trace VLAN or VXLAN use the `pktcap-uw--vlan` or `--vxlan` options. • Do not filter an IP broadcast address. • Do not use `--rcf` on ENS ports.
`--rcf-tcp-data` *`tcp_packet_data_filter`*	Capture or trace TCP data packets using the rich common filter expression. For example, to capture all HTTP/1.0 response packets with 200 OK, use the filter expression `--rcf-tcp-data "HTTP/1.0 200 OK"`. To filter on HTTP GET requests returning an index.html file, use the filter expression `--rcf-tcp-data "GET / index.html"`.

The vertical bars | represent alternative values.

Capturing Packets by Using the pktcap-uw Utility

Capture packets through the `pktcap-uw` utility in the path between a virtual switch and the physical adapters, VMkernel adapters and virtual machine adapters to troubleshoot data transfer in the network stack on an ESXi host.

Capture Packets That Arrive at a Physical Adapter

Monitor host traffic related to the external network by capturing packets at certain points in the path between a vSphere Standard Switch or vSphere Distributed Switch and a physical adapter.

You can specify a certain capture point in the data path between a virtual switch and a physical adapter, or determine a capture point by traffic direction with regard to the switch and proximity to the packet source or destination. For information about supported capture points, see Capture Points of the pktcap-uw Utility.

1. Optional: Find the name of the physical adapter that you want to monitor in the host adapter list.
   - In the vSphere Client, on the **Configure** tab for the host, expand **Networking** and select **Physical adapters**.

- In the ESXi Shell to the host, to view a list of the physical adapters and examine their state, run the following ESXCLI command:

  ```
  esxcli network nic list
  ```

  Each physical adapter is represented as `vmnicX`. *X* is the number that ESXi assigned to the physical adapter port.

2. In the ESXi Shell to the host, run the `pktcap-uw` command with the `--uplink vmnicX` argument and with options to monitor packets at a particular point, filter captured packets and save the result to a file.

   ```
   pktcap-uw--uplink vmnicX [--capturecapture_point|--dir 0|1]  [filter_options] [--outfilepcap_file_path
    [--ng]] [--countnumber_of_packets]
   ```

   where the square brackets [] enclose the options of the `pktcap-uw--uplink vmnicX` command and the vertical bars | represent alternative values.

   If you run the `pktcap-uw--uplink vmnicX` command without options, you obtain the content of packets that are incoming to the standard or distributed switch in the console output at the point where they are switched.

   a) Use the --capture option to check packets at another capture point or the --dir option at another traffic direction.

pktcap-uw Command Option	Goal
`--capture UplinkSnd`	Monitor packets immediately before they enter the physical adapter device.
`--capture UplinkRcv`	Monitor packets immediately after they are received in the network stack from the physical adapter.
`--dir 1`	Monitor packets that leave the virtual switch.
`--dir 0`	Monitor packets that enter the virtual switch.

   b) Use a *filter_options* to filter packets according to source and destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port.
   For example, to monitor packets from a source system that has IP address 192.168.25.113, use the `--srcip 192.168.25.113` filter option.

   c) Use options to save the contents of each packet or the contents of a limited number of packets to a `.pcap` or `.pcapng` file.

   - To save packets to a `.pcap` file, use the --outfile option.
   - To save packets to a `.pcapng` file, use the --ng and --outfile options.

   You can open the file in a network analyzer tool such as Wireshark.

   By default, the `pktcap-uw` utility saves the packet files to the root folder of the file system.

   d) Use the--count option to monitor only a number of packets.

3. If you have not limited the number of packets by using the --count option, press Ctrl+C to stop capturing or tracing packets.

Capture Packets That Are Received at vmnic0 from an IP Address 192.168.25.113

To capture the first 60 packets from a source system that is assigned the IP address 192.168.25.113 at vmnic0 and save them to a file called `vmnic0_rcv_srcip.pcap`, run the following `pktcap-uw` command:

```
pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile vmnic0_rcv_srcip.p-
cap --count 60
```

If the contents of the packet are saved to a file, copy the file from the host to the system that runs a graphical analyzer tool, such as Wireshark, and open it in the tool to examine the packet details.

Related Links

pktcap-uw Command Syntax for Capturing Packets on page 2336

Use the `pktcap-uw` utility to inspect the contents of packets while they traverse the network stack on an ESXi host.

pktcap-uw Options for Output Control on page 2338
Use the options for output control of the `pktcap-uw` utility to save packet contents to a file, capture up to a certain number of bytes from each packet, and limit the number of captured packets.

pktcap-uw Options for Filtering Packets on page 2339
Narrow the range of packets that you monitor by using the `pktcap-uw` utility to apply filtering options for source and destination address, VLAN, VXLAN, and next level protocol consuming the packet payload.

Trace Packets by Using the pktcap-uw Utility on page 2349
Use the `pktcap-uw` utility to trace the path that packets traverse in the network stack for latency analysis and for locating the point where a packet is corrupted or dropped.

Capture Packets for a VMXNET3 Virtual Machine Adapter

Monitor traffic that flows between a virtual switch and a VMXNET3 virtual machine adapter by using the `pktcap-uw` utility.

Verify that the virtual machine adapter is of type VMXNET3.

You can specify a certain capture point in the data path between a virtual switch and a virtual machine adapter. You can also determine a capture point by traffic direction with regard to the switch and proximity to the packet source or destination. For information about supported capture points, see Capture Points of the pktcap-uw Utility.

1. On the host, learn the port ID of the virtual machine adapter by using the `esxtop` utility.
   a) In the ESXi Shell to the host, to start the utility, run `esxtop`.
   b) To switch to the network panel of the utility, press n.
   c) In the USED-BY column, locate the virtual machine adapter, and write down the PORT-ID value for it.
      The USED-BY field contains the name of the virtual machine and the port to which the virtual machine adapter is connected.
   d) Press Q to exit `esxtop`.
2. In the ESXi Shell, run `pktcap-uw--switchport`*`port_ID`*.
   `port_ID` is the ID that the `esxtop` utility displays for the virtual machine adapter in the PORT-ID column.
3. In the ESXi Shell, run the `pktcap-uw` command with the `--switchport` *`port_ID`* argument and with options to monitor packets at a particular point, filter captured packets and save the result to a file.

   ```
   pktcap-uw--switchport port_ID [--capture capture_point|--dir 0|1 --stage 0|1]  [filter_options] [--out-
   file pcap_file_path [--ng]] [--count number_of_packets]
   ```

   where the square brackets [] enclose the options of the `pktcap-uw--switchport`*`port_ID`* command and the vertical bars | represent alternative values.

   If you run the `pktcap-uw--switchport`*`port_ID`* command without options, you obtain the content of packets that are incoming to the standard or distributed switch in the console output at the point when they are switched.

   a) To check packets at another capture point or direction in the path between the guest operating system and the virtual switch, use the --capture option or combine the values of the --dir and --stage options.

pktcap-uw Command Options	Goal
`--capture VnicTx`	Monitor packets when they pass from the virtual machine to the switch.
`--capture  VnicRx`	Monitor packets when they arrive to the virtual machine.
--dir 1--stage 0	Monitor packets immediately after they leave the virtual switch.
--dir 1	Monitor packets immediately before they enter the virtual machine.

pktcap-uw Command Options	Goal
--dir 0 --stage 1	Monitor packets immediately after they enter the virtual switch.

b) Use a *filter_options* to filter packets according to source and destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port.
For example, to monitor packets from a source system that has IP address 192.168.25.113, use the `--srcip 192.168.25.113` filter option.

c) Use options to save the contents of each packet or the contents of a limited number of packets to a `.pcap` or `.pcapng` file.

- To save packets to a `.pcap` file, use the --outfile option.
- To save packets to a `.pcapng` file, use the --ng and --outfile options.

You can open the file in a network analyzer tool such as Wireshark.

By default, the `pktcap-uw` utility saves the packet files to the root folder of the file system.

d) Use the--count option to monitor only a number of packets.

4. If you have not limited the number of packets by using the --count option, press Ctrl+C to stop capturing or tracing packets.

Capture Packets That Are Received at a Virtual Machine from an IP Address 192.168.25.113

To capture the first 60 packets from a source that is assigned the IP address 192.168.25.113 when they arrive at a virtual machine adapter with port ID 33554481 and save them to a file called `vmxnet3_rcv_srcip.pcap`, run the following `pktcap-uw` command:

```
pktcap-uw --switchport 33554481 --capture VnicRx --srcip 192.168.25.113 --outfile vmxnet3_rcv_sr-
cip.pcap --count 60
```

If the contents of the packet are saved to a file, copy the file from the host to the system that runs a graphical analyzer tool, such as Wireshark, and open it in the tool to examine the packet details.

Related Links

pktcap-uw Command Syntax for Capturing Packets on page 2336
Use the `pktcap-uw` utility to inspect the contents of packets while they traverse the network stack on an ESXi host.

pktcap-uw Options for Output Control on page 2338
Use the options for output control of the `pktcap-uw` utility to save packet contents to a file, capture up to a certain number of bytes from each packet, and limit the number of captured packets.

pktcap-uw Options for Filtering Packets on page 2339
Narrow the range of packets that you monitor by using the `pktcap-uw` utility to apply filtering options for source and destination address, VLAN, VXLAN, and next level protocol consuming the packet payload.

Trace Packets by Using the pktcap-uw Utility on page 2349
Use the `pktcap-uw` utility to trace the path that packets traverse in the network stack for latency analysis and for locating the point where a packet is corrupted or dropped.

Capture Packets for a VMkernel Adapter

Monitor packets that are exchanged between a VMkernel adapter and a virtual switch by using the `pktcap-uw` utility.

You can capture packets at a certain capture point in the flow between a virtual switch and a VMkernel adapter. You can also determine a capture point by traffic direction with regard to the switch and proximity to the packet source or destination. For information about supported capture points, see Capture Points of the pktcap-uw Utility.

1. Optional: Find the name of the VMkernel adapter that you want to monitor in the VMkernel adapter list.

- In the , expand **Networking** on the **Configure** tab for the host and select **VMkernel adapters**.

- In the ESXi Shell to the host, to view a list of the physical adapters, run the following console command:
  `esxcli network ip interface list`

Each VMkernel adapter is represented as `vmkX`, where `X` is the sequence number that ESXi assigned to the adapter.

2. In the ESXi Shell to the host, run the `pktcap-uw` command with the `--vmk vmkX` argument and with options to monitor packets at a particular point, filter captured packets and save the result to a file.

   `pktcap-uw--vmk vmkX [--capture capture_point|--dir 0|1 --stage 0|1] [filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]`

   where the square brackets [] enclose the options of the `pktcap-uw--vmk vmkX` command and the vertical bars | represent alternative values.

   You can replace the `--vmk vmkX` option with `--switchport vmkernel_adapter_port_ID`, where `vmkernel_adapter_port_ID` is the PORT-ID value that the network panel of the `esxtop` utility displays for the adapter.

   If you run the `pktcap-uw--vmk vmkX` command without options, you obtain the content of packets that are leaving the VMkernel adapter.

   a) To check transmitted or received packets at a specific place and direction, use the --capture option, or combine the values of the --dir and --stage options.

pktcap-uw Command Options	Goal
--dir 1 --stage 0	Monitor packets immediately after they leave the virtual switch.
--dir 1	Monitor packets immediately before they enter the VMkernel adapter.
--dir 0 --stage 1	Monitor packets immediately before they enter the virtual switch.

   b) Use a `filter_options` to filter packets according to source and destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port.
   For example, to monitor packets from a source system that has IP address 192.168.25.113, use the `--srcip 192.168.25.113` filter option.

   c) Use options to save the contents of each packet or the contents of a limited number of packets to a `.pcap` or `.pcapng` file.

   - To save packets to a `.pcap` file, use the --outfile option.
   - To save packets to a `.pcapng` file, use the --ng and --outfile options.

   You can open the file in a network analyzer tool such as Wireshark.

   By default, the `pktcap-uw` utility saves the packet files to the root folder of the file system.

   d) Use the--count option to monitor only a number of packets.

3. If you have not limited the number of packets by using the --count option, press Ctrl+C to stop capturing or tracing packets.

If the contents of the packet are saved to a file, copy the file from the host to the system that runs a graphical analyzer tool, such as Wireshark, and open it in the tool to examine the packet details.

Related Links

pktcap-uw Command Syntax for Capturing Packets on page 2336
Use the `pktcap-uw` utility to inspect the contents of packets while they traverse the network stack on an ESXi host.

pktcap-uw Options for Output Control on page 2338
Use the options for output control of the `pktcap-uw` utility to save packet contents to a file, capture up to a certain number of bytes from each packet, and limit the number of captured packets.

pktcap-uw Options for Filtering Packets on page 2339
Narrow the range of packets that you monitor by using the `pktcap-uw` utility to apply filtering options for source and destination address, VLAN, VXLAN, and next level protocol consuming the packet payload.

Trace Packets by Using the pktcap-uw Utility on page 2349
Use the `pktcap-uw` utility to trace the path that packets traverse in the network stack for latency analysis and for locating the point where a packet is corrupted or dropped.

Capture Dropped Packets

Troubleshoot lost connectivity by capturing dropped packets through the `pktcap-uw` utility.

A packet might be dropped at a point in the network stream for many reasons, for example, a firewall rule, filtering in an IOChain and DVfilter, VLAN mismatch, physical adapter malfunction, checksum failure, and so on. You can use the `pktcap-uw` utility to examine where packets are dropped and the reason for the drop.

1. In the ESXi Shell to the host, run the `pktcap-uw --capture Drop` command with options to monitor packets at a particular point, filter captured packets and save the result to a file.

   ```
   pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
   ```

   where the square brackets [] enclose the options of the `pktcap-uw--capture Drop` command and the vertical bars | represent alternative values.

   a) Use a *`filter_options`* to filter packets according to source and destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port.
   For example, to monitor packets from a source system that has IP address 192.168.25.113, use the `--srcip 192.168.25.113` filter option.
   b) Use options to save the contents of each packet or the contents of a limited number of packets to a `.pcap` or `.pcapng` file.

   •

   You can open the file in a network analyzer tool such as Wireshark.

   By default, the `pktcap-uw` utility saves the packet files to the root folder of the file system.

   Note: You can see the reason and the place where a packet is dropped only when you capture packets to the console output. The `pktcap-uw` utility saves only the content of packets to a `.pcap` or `.pcapng` file.
   c) Use the--count option to monitor only a number of packets.
2. If you have not limited the number of packets by using the --count option, press Ctrl+C to stop capturing or tracing packets.

Besides the contents of dropped packets, the output of the `pktcap-uw` utility displays the reason for the drop and the function in the network stack that handled the packet last.

If the contents of the packet are saved to a file, copy the file from the host to the system that runs a graphical analyzer tool, such as Wireshark, and open it in the tool to examine the packet details.

Related Links

pktcap-uw Command Syntax for Capturing Packets on page 2336
Use the `pktcap-uw` utility to inspect the contents of packets while they traverse the network stack on an ESXi host.

pktcap-uw Options for Output Control on page 2338
Use the options for output control of the `pktcap-uw` utility to save packet contents to a file, capture up to a certain number of bytes from each packet, and limit the number of captured packets.

pktcap-uw Options for Filtering Packets on page 2339

Narrow the range of packets that you monitor by using the `pktcap-uw` utility to apply filtering options for source and destination address, VLAN, VXLAN, and next level protocol consuming the packet payload.

Trace Packets by Using the pktcap-uw Utility on page 2349

Use the `pktcap-uw` utility to trace the path that packets traverse in the network stack for latency analysis and for locating the point where a packet is corrupted or dropped.

Capture Packets at DVFilter Level

Examine how packets change when they pass through a vSphere Network Appliance (DVFilter).

DVFilters are agents that reside in the stream between a virtual machine adapter and a virtual switch. They intercept packets to protect virtual machines from security attacks and unwanted traffic.

1. Optional: To find the name of the DVFilter that you want to monitor, in the ESXi Shell, run the `summarize-dvfilter` command.

   The output of the command contains the fast-path and slow-path agents of the DVFilters that are deployed on the host.

2. Run the `pktcap-uw` utility with the `--dvfilter`*`dvfilter_name`* argument and with options to monitor packets at a particular point, filter captured packets and save the result to a file.

   `pktcap-uw--dvFilter`*`dvfilter_name`*`--capture PreDVFilter|PostDVFilter [`*`filter_options`*`] [--outfile`*`p-cap_file_path`*` [--ng]] [--count`*`number_of_packets`*`]`

   where the square brackets [] enclose optional items of the `pktcap-uw--dvFilter vmnic`*`X`* command and the vertical bars | represent alternative values.

   a) Use the --capture option to monitor packets before or after the DVFilter intercepts them.

pktcap-uw Command Option	Goal
`--capture PreDVFilter`	Capture packets before they enter the DVFilter.
`--capture PostDVFilter`	Capture packets after they leave the DVFilter.

   b) Use a *`filter_options`* to filter packets according to source and destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port.
   For example, to monitor packets from a source system that has IP address 192.168.25.113, use the `--srcip 192.168.25.113` filter option.

   c) Use options to save the contents of each packet or the contents of a limited number of packets to a `.pcap` or `.pcapng` file.

   - To save packets to a `.pcap` file, use the --outfile option.
   - To save packets to a `.pcapng` file, use the --ng and --outfile options.

   You can open the file in a network analyzer tool such as Wireshark.

   By default, the `pktcap-uw` utility saves the packet files to the root folder of the file system.

   d) Use the--count option to monitor only a number of packets.

3. If you have not limited the number of packets by using the --count option, press Ctrl+C to stop capturing or tracing packets.

If the contents of the packet are saved to a file, copy the file from the host to the system that runs a graphical analyzer tool, such as Wireshark, and open it in the tool to examine the packet details.

Using the Capture Points of the pktcap-uw Utility

You use the capture points of the `pktcap-uw` utility to monitor packets when a function handles them at a specific place in the network stack on a host.

Overview of Capture Points

A capture point in the `pktcap-uw` utility represents a place in the path between a virtual switch on one side and a physical adapter, VMkernel adapter or a virtual machine adapter on the other.

You can use certain capture points in combination with an adapter option. For example, you use the UplinkRcv point when you capture uplink traffic. You can address other points standalone. For example, use the Drop point to inspect all dropped packets.

Note: Certain capture points of the `pktcap-uw` utility are designed for VMware internal use only and you should use them only under the supervision of VMware Technical Support. These capture points are not described in the *vSphere Networking* guide.

Option for Using Capture Points in the pktcap-uw Utility

To examine a packet state or content at a capture point, add the --capture*`capture_point`* option to the `pktcap-uw` utility.

Auto-Selecting a Capture Point

For traffic that is related to a physical, VMkernel or VMXNET3 adapter, by combining the --dir and --stage options you can auto-select and switch between capture points to examine how a packet changes before and after a point.

Capture Points of the pktcap-uw Utility

The `pktcap-uw` utility supports capture points that can be used only when you monitor uplink, VMkernel or virtual machine traffic, and capture points that represent special places in the stack that are not related to the adapter type.

Capture Points That Are Relevant to Physical Adapter Traffic

The `pktcap-uw--uplink vmnic`*`X`* command supports capture points for functions that handle traffic at a specific place and direction in the path between the physical adapter and the virtual switch.

Capture Point	Description
UplinkRcv	The function that receives packets from the physical adapter.
UplinkSnd	The function that sends packets to the physical adapter.
PortInput	The function that passes a list of packets from UplinkRcv to a port on the virtual switch.
PortOutput	The function that passes a list of packets from a port on the virtual switch to the UplinkSnd point.

Capture Points That Are Relevant to Virtual Machine Traffic

The `pktcap-uw--switchport`*`vmxnet3_port_ID`* command supports capture points for functions that handle traffic packets at a specific place and direction in the path between a VMXNET3 adapter and a virtual switch.

Capture Point	Description
VnicRx	The function in the virtual machine NIC backend that receives packets from the virtual switch.
VnicTx	The function in the virtual machine NIC backend that sends packets from the virtual machine to the virtual switch.
PortOutput	The function that passes a list of packets from a port on the virtual switch to Vmxnet3Rx.
PortInput	The function that passes a list of packets from Vmxnet3Tx to a port on the virtual switch. Default capture point for traffic related to a VMXNET3 adapter.

Capture Points That Are Relevant to VMkernel Adapter Traffic

The `pktcap-uw--vmk vmk`*X* and `pktcap-uw`--switchport*vmkernel_adapter_port_ID* commands support capture points that represent functions at a specific place and direction in the path between a VMkernel adapter and a virtual switch.

Capture Point	Description
PortOutput	The function that passes a list of packets from a port on the virtual switch to the VMkernel adapter.
PortInput	The function that passes a list of packets from the VMkernel adapter to a port on the virtual switch. Default capture point for traffic related to a VMkernel adapter.

Capture Points That Are Relevant to Distributed Virtual Filters

The `pktcap-uw--dvfilter`*divfilter_name* command requires a capture point that indicates whether to capture packets when they enter the DVFilter or when they leave it.

Capture Point	Description
PreDVFilter	The point before a DVFilter intercepts a packet.
PostDVFilter	The point after a DVFilter intercepts a packet.

Standalone Capture Points

Certain capture points are mapped directly to the network stack rather than to a physical, VMkernel or VMXNET3 adapter.

Capture Point	Description
Drop	Captures dropped packets and shows the place where drops occur.
TcpipDispatch	Capture packets at the function that dispatches traffic to the TCP/IP stack of the VMkernel from the virtual switch, and the reverse.
PktFree	Capture packets right before they are released.
VdrRxLeaf	Capture packets at the receive leaf I/O chain of a dynamic router in VMware NSX. Use this capture point together with the --lifID option.

Capture Point	Description
VdrRxTerminal	Capture packets at the receive terminal I/O chain of a dynamic router in VMware NSX. Use this capture point together with the --lifID option.
VdrTxLeaf	Capture packets at the transmit leaf I/O chain of a dynamic router in VMware NSX. Use this capture point together with the --lifID option.
VdrTxTerminal	Capture packets at the transmit terminal I/O chain of a dynamic router in VMware NSX. Use this capture point together with the --lifID option.

For information about dynamic routers, see the *VMware NSX* documentation.

List the Capture Points of the pktcap-uw Utility

View all capture points of the `pktcap-uw` utility to find the name of capture point for monitoring traffic at a certain place in the network stack on the ESXi host.

For information about the capture points of the `pktcap-uw` utility, see Capture Points of the pktcap-uw Utility.

In the ESXi Shell to the host, run the `pktcap-uw -A` command to view all capture points that the `pktcap-uw` utility supports.

Trace Packets by Using the pktcap-uw Utility

Use the `pktcap-uw` utility to trace the path that packets traverse in the network stack for latency analysis and for locating the point where a packet is corrupted or dropped.

The `pktcap-uw` utility shows the path of packets together with timestamps that note the time when a packet is handled by a networking function on ESXi. The utility reports the path of a packet immediately before it is released from the stack.

To view the full path information for a packet, you must print the result from the `pktcap-uw` utility in the console output or save it to a PCAPNG file.

1. In the ESXi Shell to the host, run the `pktcap-uw`--trace command with options to filter traced packets, save the result to a file and limit the number of traced packets.

   `pktcap-uw--trace [`*`filter_options`*`] [--outfile`*`pcap_file_path`*` [--ng]] [--count`*`number_of_packets`*`]`

   where the square brackets [] enclose optional items of the `pktcap-uw --trace` command and the vertical bars | represent alternative values.

   a) Use a *`filter_options`* to filter packets according to source and destination address, VLAN ID, VXLAN ID, Layer 3 protocol, and TCP port.
   For example, to monitor packets from a source system that has IP address 192.168.25.113, use the `--srcip 192.168.25.113` filter option.
   b) Use options to save the contents of each packet or the contents of a limited number of packets to a `.pcap` or `.pcapng` file.

   •

   You can open the file in a network analyzer tool such as Wireshark.

   By default, the `pktcap-uw` utility saves the packet files to the root folder of the file system.

   Note: A `.pcap` file contains only the contents of traced packets. To collect packet paths besides packet content, save the output to a `.pcapng` file.

c) Use the--count option to monitor only a number of packets.

2. If you have not limited the number of packets by using the --count option, press Ctrl+C to stop capturing or tracing packets.

If the contents of the packet are saved to a file, copy the file from the host to the system that runs a graphical analyzer tool, such as Wireshark, and open it in the tool to examine the packet details.

Related Links

Capture Packets That Arrive at a Physical Adapter on page 2340
Monitor host traffic related to the external network by capturing packets at certain points in the path between a vSphere Standard Switch or vSphere Distributed Switch and a physical adapter.

Capture Packets for a VMkernel Adapter on page 2343
Monitor packets that are exchanged between a VMkernel adapter and a virtual switch by using the `pktcap-uw` utility.

Capture Packets for a VMXNET3 Virtual Machine Adapter on page 2342
Monitor traffic that flows between a virtual switch and a VMXNET3 virtual machine adapter by using the `pktcap-uw` utility.

Capture Dropped Packets on page 2345
Troubleshoot lost connectivity by capturing dropped packets through the `pktcap-uw` utility.

Configure the NetFlow Settings of a vSphere Distributed Switch

Analyze virtual machine IP traffic that flows through a vSphere Distributed Switch by sending reports to a NetFlow collector.

vSphere Distributed Switch supports IPFIX (NetFlow version 10).

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. From the **Actions** menu, select **Settings** > **Edit Netflow**.
3. Type the **Collector IP address** and **Collector port** of the NetFlow collector.

   You can contact the NetFlow collector by IPv4 or IPv6 address.
4. Set an **Observation Domain ID** that identifies the information related to the switch.
5. To see the information from the distributed switch in the NetFlow collector under a single network device instead of under a separate device for each host on the switch, type an IPv4 address in the **Switch IP address** text box.
6. Optional: In the **Active flow export timeout** and **Idle flow export timeout** text boxes, set the time, in seconds, to wait before sending information after the flow is initiated.
7. Optional: To change the portion of data that the switch collects, configure **Sampling Rate**.

   The sampling rate represents the number of packets that NetFlow drops after every collected packet. A sampling rate of *x* instructs NetFlow to drop packets in a *collected packets*:*dropped packets* ratio 1:*x*. If the rate is 0, NetFlow samples every packet, that is, collect one packet and drop none. If the rate is 1, NetFlow samples a packet and drops the next one, and so on.
8. Optional: To collect data on network activity between virtual machines on the same host, enable **Process internal flows only**.

   Collect internal flows only if NetFlow is enabled on the physical network device to avoid sending duplicate information from the distributed switch and the physical network device.
9. Click **OK**.

Enable NetFlow reporting for traffic from virtual machines connected to a distributed port group or a port. See Manage NetFlow Monitoring on a Distributed Port Group or Distributed Port.

Working With Port Mirroring

Port mirroring allows you to mirror a distributed port's traffic to other distributed ports or specific physical switch ports.

Port mirroring is used on a switch to send a copy of packets seen on one switch port (or an entire VLAN) to a monitoring connection on another switch port. Port mirroring is used to analyze and debug data or diagnose errors on a network.

Port Mirroring Interoperability

There are some interoperability issues to consider when using vSphere port mirroring with other features of vSphere.

vMotion

vMotion functions differently depending on which vSphere port mirroring session type you select. During vMotion, a mirroring path could be temporarily invalid, but it is restored when vMotion completes.

Table 198: vMotion Interoperability with port mirroring

Port mirroring session type	Source and destination	Interoperable with vMotion	Functionality
Distributed Port Mirroring	Non-uplink distributed port source and destination	Yes	Port mirroring between distributed ports can only be local. If the source and destination are on different hosts due to vMotion, mirroring between them will not work. However, if the source and destination move to the same host, port mirroring works.
Remote Mirroring Source	Non-uplink distributed port source	Yes	When a source distributed port is moved from host A to host B, the original mirroring path from the source port to A's uplink is removed on A, and a new mirroring path from the source port to B's uplink is created on B. Which uplink is used is determined by the uplink name specified in session.
	Uplink port destinations	No	Uplinks can not be moved by vMotion.
Remote Mirroring Destination	VLAN source	No	
	Non-uplink distributed port destination	Yes	When a destination distributed port is moved from host A to host B, all original mirroring paths from source VLANs to the destination port are moved from A to B.
Encapsulated Remote Mirroring (L3) Source	Non-uplink distributed port source	Yes	When a source distributed port is moved from host A to host B, all original mirroring paths from the source port to destination IPs are moved from A to B.
	IP destination	No	

Port mirroring session type	Source and destination	Interoperable with vMotion	Functionality
Distributed Port Mirroring (legacy)	IP source	No	
	Non-uplink distributed port destination	No	When a destination distributed port is moved from host A to host B, all original mirroring paths from source IPs to the destination port are invalid because the port mirroring session source still sees the destination on A.

TSO and LRO

TCP Segmentation Offload (TSO) and large receive offload (LRO) might cause the number of mirroring packets to not equal to the number of mirrored packets.

When TSO is enabled on a vNIC, the vNIC might send a large packet to a distributed switch. When LRO is enabled on a vNIC, small packets sent to it might be merged into a large packet.

Source	Destination	Description
TSO	LRO	Packets from the source vNIC might be large packets, and whether they are split is determined by whether their sizes are larger than the destination vNIC LRO limitation.
TSO	Any destination	Packets from the source vNIC might be large packets, and they are split to standard packets at the destination vNIC.
Any source	LRO	Packets from the source vNIC are standard packets, and they might be merged into larger packets at the destination vNIC.

Create a Port Mirroring Session

Create a port mirroring session by using the vSphere Client to mirror vSphere Distributed Switch traffic to ports, uplinks, and remote IP addresses.

Verify that the vSphere Distributed Switch is version 5.0.0 and later.

Select Port Mirroring Session Type

To begin a port mirroring session, you must specify the type of port mirroring session.

1. Browse to a distributed switch in the vSphere Client navigator.
2. Click the **Configure** tab and expand **Settings**.
3. Select the **Port mirroring** option and click **New**.
4. Select the session type for the port mirroring session.

   Note:

   When the session type for the port mirroring session is set to **Distributed Port Mirroring**, **Remote Mirror Source**, or **Remote Mirror Destination**, the switching VLAN tag will not be in the mirrored packets.

Option	Description
Distributed Port Mirroring	Mirror packets from a number of distributed ports to other distributed ports on the same host. If the source and the destination are on different hosts, this session type does not function.
Remote Mirroring Source	Mirror packets from a number of distributed ports to specific uplink ports on the corresponding host.
Remote Mirroring Destination	Mirror packets from a number of VLANs to distributed ports.
Encapsulated Remote Mirroring (L3) Source	Mirror packets from a number of distributed ports to the IP addresses of a remote agent. The virtual machine's traffic is mirrored to a physical or virtual destination through an IP tunnel.

5. Click **Next**.

Specify Port Mirroring Name and Session Details

To continue creating a port mirroring session, specify the name, description, and session details for the new port mirroring session.

1. Set the session properties. Different options are available for configuration depending on which session type you selected.

Option	Description
Name	You can enter a unique name for the port mirroring session, or accept the automatically generated session name.
Status	Use the drop down menu to enable or disable the session.
Session type	Displays the type of session you selected.
Encapsulation Type	Select **GRE**, **ERSPAN TWO**, or **ERSPAN THREE**. **Note:** This option is enabled when session type is set to **Encapsulated Remote Mirroring (L3) Source**.
Session ID	Specify an ERSPAN ID if encapsulation type is set to **ERSPAN TWO** or **ERSPAN THREE**. **Note:** This option is enabled when session type is set to **Encapsulated Remote Mirroring (L3) Source**.
Encapsulation VLAN ID	VLAN ID that encapsulates all frames at the destination ports.

Option	Description
	Note: If the original frames have a VLAN and Preserve original VLAN is not selected, the encapsulation VLAN replaces the original VLAN. This option is enabled when session type is set to **Remote Mirroring Source**.
Preserve original VLAN	Select Preserve original VLAN to keep the original VLAN in an inner tag so mirrored frames are double encapsulated. This option is enabled when session type is set to **Remote Mirroring Source**.
Normal I/O on destination ports	Use the drop-down menu to allow or disallow normal I/O on destination ports. This property is only available for uplink and distributed port destinations. If you disallow this option, mirrored traffic will be allowed on outgoing destination ports, but incoming traffic will not be allowed.
TCP/IP Stack	Use the drop down menu to select the type of TCP/IP stack. • Default: The default TCP/IP stack. • Mirror: Using mirror stack instead of default TCP/IP netstack can separate mirror traffic from management traffic. Without mirror stack, mirror traffic is bound to default TCP/IP stack. The management traffic also uses the default TCP/IP stack. If the mirror traffic is large, then it affects the management traffic. If you want to separate the mirror traffic from the default TCP/IP stack, then you can have a dedicated mirror netstack on the ESXi. You can enable this dedicated netstack while configuring Encapsulated Remote Mirroring sessions. **Note:** This option is enabled when session type is set to **Encapsulated Remote Mirroring (L3) Source**.
Mirrored packet length (Bytes)	Use the check box to enable mirrored packet length in bytes. This puts a limit on the size of mirrored frames. If this option is selected, all mirrored frames are truncated to the specified length.
Sampling rate	Select the rate at which packets are sampled. This is enabled by default for all port mirroring sessions except legacy sessions.
Description	You have the option to enter a description of the port mirroring session configuration.

2. Click **Next**.

Select Port Mirroring Sources

To continue creating a port mirroring session, select sources and traffic direction for the new port mirroring session.

You can create a port mirroring session without setting the source and destinations. When a source and destination are not set, a port mirroring session is created without the mirroring path. This allows you to create a port mirroring session with the correct properties set. Once the properties are set, you can edit the port mirroring session to add the source and destination information.

Note: Consider the following limitations when selecting port mirroring sources.

- A source mirror port cannot be used in more than one mirror session.
- A port cannot be used as a mirror source and mirror destination in the same or different mirror sessions at the same time.

1. Select the source of the traffic to be mirrored and the traffic direction.

   Depending on the type of port mirroring session you selected, different options are available for configuration.

Option	Description
Add existing ports from a list	Click **Select distributed ports**. A dialog box displays a list of existing ports. Select the check box next to the distributed port and click **OK**. You can choose more than one distributed port.
Add existing ports by port number	Click **Add distributed ports**, enter the port number and click **OK.**
Set the traffic direction	After adding ports, select the port in the list and click the ingress, egress, or ingress/egress button. Your choice appears in the Traffic Direction column.
Specify the source VLAN	If you selected a Remote Mirroring Destination sessions type, you must specify the source VLAN. Click **Add** to add a VLAN ID. Edit the ID by using the up and down arrows, or by clicking in the field and entering the VLAN ID manually.

2. Click **Next**.

Select Port Mirroring Destinations and Verify Settings

To complete the creation of a port mirroring session, select ports or uplinks as destinations for the port mirroring session.

You can create a port mirroring session without setting the source and destinations. When a source and destination are not set, a port mirroring session is created without the mirroring path. This allows you to create a port mirroring session with the correct properties set. Once the properties are set, you can edit the port mirroring session to add the source and destination information.

Port mirroring is checked against the VLAN forwarding policy. If the VLAN of the original frames is not equal to or trunked by the destination port, the frames are not mirrored.

1. Select the destination for the port mirroring session.

   Depending on which type of session you chose, different options are available.

Option	Description
Select a destination distributed port	Click **Select distributed ports** to select ports from a list, or click **Add distributed ports** to add ports by port number. You can add more than one distributed port.
Select an uplink	Select an available uplink from the list and click **Add** to add the uplink to the port mirroring session. You can select more than one uplink.
Select ports or uplinks	Click **Select distributed ports** to select ports from a list, or click **Add distributed ports** to add ports by port number. You can add more than one distributed port. Click **Add uplinks** to add uplinks as the destination. Select uplinks from the list and click **OK**.
Specify IP address	Click **Add**. A new list entry is created. Select the entry and either click **Edit** to enter the IP address, or click directly in the IP Address field and type the IP address. A warning appears if the IP address is invalid.

2. Click **Next**.
3. Review the information that you entered for the port mirroring session on the **Ready to complete** page.
4. Optional: Use the **Back** button to edit the information.
5. Click **Finish**.

The new port mirroring session appears in the Port Mirroring section of the **Settings** tab.

View Port Mirroring Session Details

View port mirroring session details, including status, sources, and destinations.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and click **Port mirroring**.
3. Select a port mirroring session from the list to display more detailed information at the bottom of the screen. Use the tabs to review configuration details.
4. Optional: Click **New** to add a new port mirroring session.
5. Optional: Click **Edit** to edit the details for the selected port mirroring session.
6. Optional: Click **Remove** to delete the selected port mirroring session.

Edit Port Mirroring Session Details, Sources, and Destinations

Edit the details of a port mirroring session, including name, description, status, sources, and destinations.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Configure** tab, expand **Settings** and click **Port mirroring**.
3. Select a port mirroring session from the list and click **Edit**.
4. On the **Properties** page, edit the session properties.
   Depending on the type of port mirroring session being edited, different options are available for configuration.

Option	Description
Name	You can enter a unique name for the port mirroring session, or accept the automatically generated session name.
Status	Use the drop-down menu to enable or disable the session.
Normal I/O on destination ports	Use the drop-down menu to allow or disallow normal I/O on destination ports. This property is only available for uplink and distributed port destinations. If you do not select this option, mirrored traffic will be allowed out on destination ports, but no traffic will be allowed in.
Sampling rate	Select the rate at which packets are sampled. This is enabled by default for all port mirroring sessions except legacy sessions.
Mirrored packet length (Bytes)	Use the check box to enable mirrored packet length in bytes. This puts a limit on the size of mirrored frames. If this option is selected, all mirrored frames are truncated to the specified length.
Description	You have the option to enter a description of the port mirroring session configuration.

5. On the **Sources** page, edit sources for the port mirroring session.
   Depending on the type of port mirroring session being edited, different options are available for configuration.

Option	Description
Add existing ports from a list	Click the **Select distributed ports to add to this port mirroring session.** button. A dialog opens with a list of existing ports. Select the check box next to the distributed port and click **OK**. You can choose more than one distributed port.
Set the traffic direction	After adding ports, select the port in the list and click the ingress, egress, or ingress/egress button. Your choice is displayed in the Traffic Direction column.

6. In the **Destinations** section, edit the destinations for the port mirroring session.
   Depending on the type of port mirroring session being edited, different options are available for configuration.

Option	Description
Select a destination distributed port	Click the **Select distributed portsto add to this port mirroring session.** button to select ports from a list. You can add more than one distributed port.

7. Click **OK**.

vSphere Distributed Switch Health Check

The health check support helps you identify and troubleshoot configuration errors in a vSphere Distributed Switch.

Use vSphere Distributed Switch health check to examine certain settings on the distributed and physical switches to identify common errors in your environment's networking configuration. The default interval between two health checks is 1 minute.

Important: Use health check to troubleshoot network problems, and then disable it after you identify and resolve the problem. After you disable vSphere Distributed Switch health check, the generated MAC addresses age out of your physical network environment according to your network policy. For more information, see Knowledge Base article KB 2034795.

Configuration Error	Health Check	Required Configuration on the Distributed Switch
The VLAN trunk ranges configured on the distributed switch do not match the trunk ranges on the physical switch.	Checks whether the VLAN settings on the distributed switch match the trunk port configuration on the connected physical switch ports.	At least two active physical NICs
The MTU settings on the physical network adapters, distributed switch, and physical switch ports do not match.	Checks whether the physical access switch port MTU jumbo frame setting based on per VLAN matches the vSphere distributed switch MTU setting.	At least two active physical NICs
The teaming policy configured on the port groups does not match the policy on the physical switch port-channel.	Checks whether the connected access ports of the physical switch that participate in an EtherChannel are paired with distributed ports whose teaming policy is set to IP hash.	At least two active physical NICs and two hosts

Health check is limited to only the access switch port to which the distributed switch uplink connects.

Manage vSphere Distributed Switch Health Check

Health check monitors for changes in vSphere Distributed Switch configurations. You must enable vSphere Distributed Switch health check to perform checks on distributed switch configurations.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. Select the **Configure** tab and expand Setting.
3. Select **Health Check** and click the **Edit** button.
4. Use the drop-down menus to enable or disable health check options.

Option	Description
VLAN and MTU	Reports the status of distributed uplink ports and VLAN ranges.
Teaming and Failover	Checks for any configuration mismatch between the ESXi host and the physical switch used in the teaming policy.

5. Click **OK**.

When you change the configuration of a vSphere Distributed Switch, you can view information about the change in the **Monitor** tab in the vSphere Client. See View vSphere Distributed Switch Health Status.

View vSphere Distributed Switch Health Status

Once you have enabled health check on a vSphere Distributed Switch, you can view the network health status of the hosts connected in the vSphere Client .

Verify that health check for VLAN and MTU, and for teaming policy is enabled on the vSphere Distributed Switch. See Manage vSphere Distributed Switch Health Check.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. On the **Monitor** tab, click **Health**.
3. In the Host member health status section, examine the overall, VLAN, MTU and teaming health of the hosts connected to the switch.

Switch Discovery Protocol

Switch discovery protocols help vSphere administrators to determine which port of the physical switch is connected to a vSphere standard switch or vSphere distributed switch.

vSphere 5.0 and later supports Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP). CDP is available for vSphere standard switches and vSphere distributed switches connected to Cisco physical switches. LLDP is available for vSphere distributed switches version 5.0.0 and later.

When CDP or LLDP is enabled for a particular vSphere distributed switch or vSphere standard switch, you can view properties of the peer physical switch such as device ID, software version, and timeout from the vSphere Client.

Enable Cisco Discovery Protocol on a vSphere Distributed Switch

Cisco Discovery Protocol (CDP) enables vSphere administrators to determine which port of a physical Cisco switch connects to a vSphere Standard Switch or vSphere Distributed Switch. When CDP is enabled for a vSphere Distributed Switch, you can view the properties of the Cisco switch such as device ID, software version, and timeout.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. From the **Actions** menu, select **Settings** > **Edit Settings**.
3. In the Edit Settings dialog box, click **Advanced**.
4. In the Discovery Protocol section, select **Cisco Discovery Protocol** from the **Type** drop-down menu.
5. From the **Operation** drop-down menu, select the operational mode of the ESXi hosts connected to the switch.

Option	Description
Listen	ESXi detects and displays information about the associated Cisco switch port, but information about the vSphere Distributed Switch is not available to the Cisco switch administrator.
Advertise	ESXi makes information about the vSphere Distributed Switch available to the Cisco switch administrator, but does not detect and display information about the Cisco switch.
Both	ESXi detects and displays information about the associated Cisco switch and makes information about the vSphere Distributed Switch available to the Cisco switch administrator.

6. Click **OK**.

Enable Link Layer Discovery Protocol on a vSphere Distributed Switch

With Link Layer Discovery Protocol (LLDP), vSphere administrators can determine which physical switch port connects to a given vSphere Distributed Switch. When LLDP is enabled for a particular distributed switch, you can view properties of the physical switch (such as chassis ID, system name and description, and device capabilities) from the .

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. From the **Actions** menu, select **Settings** > **Edit Settings**.
3. In the Edit Settings dialog box, click **Advanced**.
4. In the Discovery Protocol section, select **Link Layer Discovery Protocol** from the **Type** drop-down menu.
5. From the **Operation** drop-down menu, select the operational mode of the ESXi hosts connected to the switch.

Operation	Description
Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere Distributed Switch is not available to the switch administrator.
Advertise	ESXi makes information about the vSphere Distributed Switch available to the switch administrator, but does not detect and display information about the physical switch.
Both	ESXi detects and displays information about the associated physical switch and makes information about the vSphere Distributed Switch available to the switch administrator.

6. Click **OK**.

View Switch Information

When Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) is enabled on the distributed switch and the hosts connected to the switch are in Listen or Both operational mode, you can view physical switch information from the vSphere Client.

1. In the , navigate to the host.
2. On the **Configure** tab, expand **Networking** and click **Physical adapters**.
3. Select a physical adapter from the list to view its detailed information.

According to the enabled switch discovery protocol, the properties of the switch appear under the **CDP** or **LLDP** tab. If the information is available in the network, under Peer device capability you can examine the system capabilities of the switch.

View the Topology Diagram of an NSX Virtual Distributed Switch

You can examine the structure and components of an NSX Virtual Distributed Switch (N-VDS) by viewing its topology diagram.

The topology diagram of an N-VDS provides a visual representation of the adapters and port groups connected to the switch.

From the diagram you can view the settings of a selected port group and of a selected adapter.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **Networking** and select **Virtual Switches**.
3. Select the N-VDS from the list.

The diagram appears under the list of virtual switches on the host.

You can use the topology diagram to examine whether a virtual machine or VMkernel adapter is connected to the external network and to identify the physical adapter that carries the data.

Configuring Protocol Profiles for Virtual Machine Networking

A network protocol profile contains a pool of IPv4 and IPv6 addresses that vCenter Server assigns to vApps or to virtual machines with vApp functionality that are connected to port groups associated with the profile.

Network protocol profiles also contain settings for the IP subnet, DNS, and HTTP proxy server.

To configure the networking settings of virtual machines by using from network protocol profiles, perform the following operations:

- Create network profiles at the level of a data center or a vSphere distributed switch.
- Associate a protocol profile with the port group of a vApp virtual machine.
- Enable the transient or static IP allocation policy from the settings of the vApp or from the vApp options of a virtual machine.

Note: If you move a vApp or a virtual machine that retrieves its network settings from a protocol profile to another data center, to power it on you must assign a protocol profile to the connected port group on the destination data center.

Add a Network Protocol Profile

A network protocol profile contains a pool of IPv4 and IPv6 addresses. vCenter Server assigns those resources to vApps or to the virtual machines with vApp functionality that are connected to the port groups associated with the profile.

You can configure network protocol profile ranges for IPv4, IPv6, or both. vCenter Server uses these ranges to dynamically allocate IP addresses to the virtual machines within a vApp, when the vApp uses transient IP allocation policy.

Network protocol profiles also contain settings for the IP subnet, the DNS, and HTTP proxy servers.

Note: If you move a vApp or a virtual machine that retrieves its network settings from a protocol profile to another data center, to power on the vApp or virtual machine you must assign a protocol profile to the connected port group on the destination data center.

1. Navigate to a data center that is associated with a vApp.
2. On the **Configure** tab, select **More** > **Network Protocol Profiles**.

   Existing network protocol profiles are listed.
3. Click the **Add** button.

   The **Add Network Protocol Profile** wizard opens.
4. On the **Name and network** page, enter the name of the network protocol profile and select the networks that use this profile. Click **Next**.

   A network can be associated with one network protocol profile at a time.

5. On the **IPv4** page, configure the relevant IPv4 settings.
   a) In the **Subnet** and the **Gateway** text boxes, enter the IP subnet and gateway.
   b) To indicate that the DHCP server is available on the network, select the **DHCP Present** radio button.
   c) In the **DNS server addresses** text box, enter the DNS server information.
   d) To specify an IP pool range, enable the **IP Pool** option.
   e) If you enable IP pools, enter a comma-separated list of host address ranges in the **IP pool range** text box.

      A range consists of an IP address, a pound sign (#), and a number indicating the length of the range.

      For example, `10.20.60.4#10, 10.20.61.0#2` indicates that the IPv4 addresses can range from 10.20.60.4 to 10.20.60.13 and 10.20.61.0 to 10.20.61.1.

      The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** text box cannot include the gateway address.
   f) Click **Next**.
6. On the **IPv6** page, configure the relevant IPv6 settings.
   a) In the **Subnet** and the **Gateway** text boxes, enter the IP subnet and gateway.
   b) Select the **DHCP Present** radio button to indicate that the DHCP server is available on this network.
   c) In the **DNS server addresses**, enter the DNS server information.
   d) Enable the **IP Pool** option to specify an IP pool range.
   e) If you enable IP pools, enter a comma-separated list of host address ranges in the **IP pool range** text box.

      A range consists of an IP address, a pound sign (#), and a number indicating the length of the range.

      For example, assume that you specify the following IP pool range: `fe80:0:0:0:2bff:fe59:5a:2b#10, fe80:0:0:0:2bff:fe59:5f:b1#2`. Then the addresses are in this range:

      fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

      and

      fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2 .

      The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** text box cannot include the gateway address.
   f) Click **Next**.
7. On the **Other network configurations** page, specify additional network configurations.
   a) Enter the DNS domain.
   b) Enter the host prefix.
   c) Enter the DNS search path.

      The search paths are specified as a list of DNS domains separated by commas, semi-colons, or spaces.
   d) Enter the server name and port number for the proxy server.

      The server name must include a colon and a port number. For example, `web-proxy:3912` is a valid proxy server.
   e) Click **Next**.
8. On the **Name and Network Assignment** page, review the settings and click **Finish**.

Related Links

Associate a Port Group with a Network Protocol Profile on page 2364

To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp on page 2365

After you associate a network protocol profile with a port group of a standard switch or a distributed switch, you can use the profile to dynamically allocate IP addresses to a virtual machine that is within a vApp.

Select the Network Protocol Profile Name and Network

Name the network protocol profile and select the network that should use it.

1. Type the name of the network protocol profile.
2. Select the networks that use this network protocol profile.
   A network can be associated with one network protocol profile at a time.
3. Click **Next**.

Specify Network Protocol Profile IPv4 Configuration

A network protocol profile contains a pool of IPv4 and IPv6 addresses for use by vApps. When you create a network protocol profile, you set up its IPv4 configuration.

You can configure network protocol profile ranges for IPv4, IPv6, or both. vCenter Server uses these ranges to dynamically allocate IP addresses to virtual machines when a vApp is set up to use transient IP allocation.

1. Enter the **IP Subnet** and **Gateway** in their respective fields.
2. Select **DHCP Present** to indicate that the DHCP server is available on this network.
3. Enter the DNS server information.
   Specify the servers by IP addresses separated by a comma, semicolon, or space.
4. Select the **Enable IP Pool** check box to specify an IP pool range.
5. If you enable IP Pools, enter a comma-separated list of host address ranges in the **IP pool range** field.
   A range consists of an IP address, a pound sign (#), and a number indicating the length of the range.

   The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** field cannot include the gateway address.

   For example, `10.20.60.4#10, 10.20.61.0#2` indicates that the IPv4 addresses can range from 10.20.60.4 to 10.20.60.13 and 10.20.61.0 to 10.20.61.1.
6. Click **Next**.

Specify Network Protocol Profile IPv6 Configuration

A network protocol profile contains a pool of IPv4 and IPv6 addresses for use by vApps. When you create a network protocol profile, you set up its IPv6 configuration.

You can configure network protocol profile ranges for IPv4, IPv6, or both. vCenter Server uses these ranges to dynamically allocate IP addresses to virtual machines when a vApp is set up to use transient IP allocation.

1. Enter the **IP Subnet** and **Gateway** in their respective fields.
2. Select **DHCP Present** to indicate that the DHCP server is available on this network.
3. Enter the DNS server information.
   Specify the servers by IP addresses separated by a comma, semicolon, or space.

4. Select the **Enable IP Pool** check box to specify an IP pool range.
5. If you enable IP Pools, enter a comma-separated list of host address ranges in the **IP pool range** field.

   A range consists of an IP address, a pound sign (#), and a number indicating the length of the range. For example, assume that you specify the following IP pool range:

   fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2

   Then the addresses are in this range:

   fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

   and

   fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2

   The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** field cannot include the gateway address.
6. Click **Next**.

Specify Network Protocol Profile DNS and Other Configuration

When you create a network protocol profile, you can specify the DNS domain, DNS search path, a host prefix, and HTTP proxy.

1. Enter the DNS domain.
2. Enter the host prefix.
3. Enter the DNS search path.

   The search paths are specified as a list of DNS domains separated by commas, semi-colons, or spaces.
4. Enter the server name and port number for the proxy server.

   The server name can optionally include a colon and a port number.

   For example, `web-proxy:3912` is a valid proxy server.
5. Click **Next**.

Complete the Network Protocol Profile Creation

Review the settings and click **Finish** to complete adding the network protocol profile.

Associate a Port Group with a Network Protocol Profile

To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

You can associate a port group of a standard switch or a distributed port group of a distributed switch with a network protocol profile by using the settings of the group.

1. Navigate to a distributed port group of a vSphere Distributed Switch or to a port group of a vSphere Standard Switch in the Networking view of the vSphere Client.

   The port groups of standard switches are under the data center. The vSphere Client displays distributed port groups under the parent distributed switch object.
2. On the **Configure** tab, expand **More** and click **Network Protocol Profiles**.
3. Click **Associate a network protocol profile with the selected network** icon in the upper right corner.

   The **Associate Network Protocol Profile** wizard opens.

4. On the Set association type page, select **Use an existing network protocol profile** and click **Next**.

   If the existing network protocol profiles do not contain settings suitable for the vApp virtual machines in the port group, you must create a new profile.

5. On the Choose existing network protocol profile page, select the network protocol profile and click **Next**.
6. On the Ready to complete page, review the association and settings of the network protocol profile, and click **Finish**.

Related Links

Add a Network Protocol Profile on page 2361

A network protocol profile contains a pool of IPv4 and IPv6 addresses. vCenter Server assigns those resources to vApps or to the virtual machines with vApp functionality that are connected to the port groups associated with the profile.

Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp on page 2365

After you associate a network protocol profile with a port group of a standard switch or a distributed switch, you can use the profile to dynamically allocate IP addresses to a virtual machine that is within a vApp.

Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine or vApp

After you associate a network protocol profile with a port group of a standard switch or a distributed switch, you can use the profile to dynamically allocate IP addresses to a virtual machine that is within a vApp.

Verify that the virtual machine is connected to a port group that is associated with the network protocol profile.

Select your task.

Option	Description
Use a Network Protocol Profile to Allocate IP Addresses to a Virtual Machine	1. Navigate to a virtual machine in the vCenter Server inventory. 2. On the **Configure tab**, expand **Settings** and select **vApp Options**. 3. Click the **Edit** button. The **Edit vApp options** dialog box opens. 4. If vApp options are not enabled, select the **Enable vApp options** check box. 5. Click the **IP Allocation** tab. 6. In the Authoring section, select **OVF environment** as an IP allocation scheme. 7. In the Deployment section, set the **IP allocation** to **Transient - IP Pool** or **Static - IP Pool**. 8. Click **OK**.
Use a Network Protocol Profile to Allocate IP Addresses to a vApp	1. Navigate to a vApp in the vCenter Server inventory 2. Right-click the vApp and select **Edit Settings**. The **Edit vApp** dialog box opens. 3. Click the **IP Allocation** tab. 4. In the Authoring section, select **OVF environment** as an IP allocation scheme. 5. In the Deployment section, set the **IP allocation** to **Transient - IP Pool** or **Static - IP Pool**. 6. Click **OK**.

Both the **Static - IP Pool** and **Transient - IP Pool** options allocate an IP address from the range defined in the network protocol profile that is associated with the port group. If you select **Static - IP Pool**, the IP address is assigned the first time the virtual machine or vApp is powered on. The assigned IP address persists across restarts. If you select **Transient - IP Pool**, an IP address is assigned every the virtual machine or vApp is powered on.

When the virtual machine is powered on, the adapters connected to the port group receive IP addresses from the range in the protocol profile. When the virtual machine is powered off, the IP addresses are released.

Related Links

Add a Network Protocol Profile on page 2361

A network protocol profile contains a pool of IPv4 and IPv6 addresses. vCenter Server assigns those resources to vApps or to the virtual machines with vApp functionality that are connected to the port groups associated with the profile.

Associate a Port Group with a Network Protocol Profile on page 2364

To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

Multicast Filtering

In vSphere 6.0 and later, vSphere Distributed Switch supports basic and snooping models for filtering of multicast packets that are related to individual multicast groups. Choose a model according to the number of multicast groups to which the virtual machines on the switch subscribe.

Multicast Filtering Modes

In addition to the default basic mode for filtering multicast traffic, vSphere Distributed Switch 6.0.0 and later releases support multicast snooping that forwards multicast traffic in a more precise way based on the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) messages from virtual machines.

Basic Multicast Filtering

In basic multicast filtering mode, a vSphere Standard Switch or vSphere Distributed Switch forwards multicast traffic for virtual machines according to the destination MAC address of the multicast group. When joining a multicast group, the guest operating system pushes the multicast MAC address of the group down to the network through the switch. The switch saves the mapping between the port and the destination multicast MAC address in a local forwarding table.

The switch does not interpret the IGMP messages that a virtual machine sends to join or leave a group. The switch sends them directly to the local multicast router, which then interprets them to join the virtual machine to or remove it from the group.

The basic mode has the following restrictions:

- A virtual machine might receive packets from groups that it is not subscribed for because the switch forwards packets according to the destination MAC address of a multicast group, which can be potentially mapped up to 32 IP multicast groups.
- A virtual machine that is subscribed for traffic from more than 32 multicast MAC addresses receives packets that it is not subscribed for because of a limitation in the forwarding model.
- The switch does not filter packets according to source address as defined in IGMP version 3.

Multicast Snooping

In multicast snooping mode, a vSphere Distributed Switch provides IGMP and MLD snooping according to RFC 4541. The switch dispatches multicast traffic more precisely by using IP addresses. This mode supports IGMPv1, IGMPv2, and IGMPv3 for IPv4 multicast group addresses, and MLDv1 and MLDv2 for IPv6 multicast group addresses.

The switch dynamically detects the membership of a virtual machine. When a virtual machine sends a packet which contains IGMP or MLD membership information through a switch port, the switch creates a record about the destination IP address of the group, and in the case of IGMPv3, about a source IP address that the virtual machine prefers to receive traffic from. If a virtual machine does not renew its membership to a group within a certain period of time, the switch removes the entry for the group from the lookup records.

In multicast snooping mode of a distributed switch, a virtual machine can receive multicast traffic on a single switch port from up to 512 groups and 10 sources.

Note: In vSphere 6.7, the default multicast filtering mode is Basic. In vSphere 7.0, the default multicast filtering mode is IGMP/MLD snooping. When the DVS is upgraded to 7.0, the default multicast filtering mode will change from basic to IGMP/MLD snooping.

Related Links

Enable Multicast Snooping on a vSphere Distributed Switch on page 2367
Use multicast snooping on a vSphere Distributed Switch to forward traffic in a precise manner according to Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) membership information that virtual machines send to subscribe for multicast traffic.

Edit the Query Time Interval for Multicast Snooping on page 2368
When IGMP or MLD multicast snooping is enabled on a vSphere Distributed Switch, the switch sends general queries about the membership of virtual machines in case a snooping querier is not configured on the physical switch. On ESXi hosts that are attached to the distributed switch, you can edit the time interval in which the switch sends general queries.

Edit the Number of Source IP Addresses for IGMP and MLD on page 2368
When you enable IGMP or MLD multicast snooping on a vSphere Distributed Switch, you can edit the maximum number of IP sources from which the members of a multicast group receive packets.

Enable Multicast Snooping on a vSphere Distributed Switch

Use multicast snooping on a vSphere Distributed Switch to forward traffic in a precise manner according to Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) membership information that virtual machines send to subscribe for multicast traffic.

Verify that vSphere Distributed Switch is version 6.0.0 and later.

Use multicast snooping if virtualized workloads on the switch subscribe to more than 32 multicast groups or must receive traffic from specific source nodes. For information about the multicast filtering modes of vSphere Distributed Switch, see Multicast Filtering Modes.

1. On the vSphere Client Home page, click **Networking** and navigate to the distributed switch.
2. From the **Actions** menu, select **Settings** > **Edit Settings**.
3. In the dialog box that displays the settings of the switch, click **Advanced**.
4. From the **Multicast filtering mode** drop-down menu, select **IGMP/MLD snooping**, and click **OK**.

Multicast snooping becomes active on hosts running ESXi 6.0 and later.

Related Links

Multicast Filtering Modes on page 2366
In addition to the default basic mode for filtering multicast traffic, vSphere Distributed Switch 6.0.0 and later releases support multicast snooping that forwards multicast traffic in a more precise way based on the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) messages from virtual machines.

Edit the Query Time Interval for Multicast Snooping on page 2368
When IGMP or MLD multicast snooping is enabled on a vSphere Distributed Switch, the switch sends general queries about the membership of virtual machines in case a snooping querier is not configured on the physical switch. On ESXi hosts that are attached to the distributed switch, you can edit the time interval in which the switch sends general queries.

Edit the Number of Source IP Addresses for IGMP and MLD on page 2368
When you enable IGMP or MLD multicast snooping on a vSphere Distributed Switch, you can edit the maximum number of IP sources from which the members of a multicast group receive packets.

Edit the Query Time Interval for Multicast Snooping

When IGMP or MLD multicast snooping is enabled on a vSphere Distributed Switch, the switch sends general queries about the membership of virtual machines in case a snooping querier is not configured on the physical switch. On ESXi hosts that are attached to the distributed switch, you can edit the time interval in which the switch sends general queries.

The default time interval for sending snooping queries is 125 seconds.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **System** and select **Advanced System Settings**.
3. Click **Edit**.
4. Locate the `Net.IGMPQueryInterval` system setting and enter a new value in seconds for the setting.
5. Click **OK**

Related Links

Multicast Filtering Modes on page 2366
In addition to the default basic mode for filtering multicast traffic, vSphere Distributed Switch 6.0.0 and later releases support multicast snooping that forwards multicast traffic in a more precise way based on the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) messages from virtual machines.

Enable Multicast Snooping on a vSphere Distributed Switch on page 2367
Use multicast snooping on a vSphere Distributed Switch to forward traffic in a precise manner according to Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) membership information that virtual machines send to subscribe for multicast traffic.

Edit the Number of Source IP Addresses for IGMP and MLD on page 2368
When you enable IGMP or MLD multicast snooping on a vSphere Distributed Switch, you can edit the maximum number of IP sources from which the members of a multicast group receive packets.

Edit the Number of Source IP Addresses for IGMP and MLD

When you enable IGMP or MLD multicast snooping on a vSphere Distributed Switch, you can edit the maximum number of IP sources from which the members of a multicast group receive packets.

1. In the vSphere Client, navigate to the host.
2. On the **Configure** tab, expand **System** and select **Advanced System Settings**.
3. Click **Edit**.
4. Locate the `Net.IGMPV3MaxSrcIPNum` or `Net.MLDV2MaxSrcIPNum` system settingand enter a new value between 1 and 32 for the setting.
5. Click **OK**.

Related Links

Multicast Filtering Modes on page 2366
In addition to the default basic mode for filtering multicast traffic, vSphere Distributed Switch 6.0.0 and later releases support multicast snooping that forwards multicast traffic in a more precise way based on the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) messages from virtual machines.

Enable Multicast Snooping on a vSphere Distributed Switch on page 2367
Use multicast snooping on a vSphere Distributed Switch to forward traffic in a precise manner according to Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) membership information that virtual machines send to subscribe for multicast traffic.

Edit the Query Time Interval for Multicast Snooping on page 2368

When IGMP or MLD multicast snooping is enabled on a vSphere Distributed Switch, the switch sends general queries about the membership of virtual machines in case a snooping querier is not configured on the physical switch. On ESXi hosts that are attached to the distributed switch, you can edit the time interval in which the switch sends general queries.

What is Stateless Network Deployment

Stateless is a mode of execution for ESXi hosts with no local storage that formerly would save configuration or state. Configurations are abstracted into a host profile, which is a template that applies to a class of machines. Stateless allows easy replacement, removal, and addition of failed hardware, and improves the ease of scaling a hardware deployment.

Every stateless ESXi boot is like a first boot. The ESXi host boots with networking connectivity to vCenter Server through the built-in standard switch. If the host profile specifies distributed switch membership, vCenter Server joins the ESXi host to VMware distributed switches.

When planning the network setup for stateless ESXi hosts, you should keep the configuration as generic as possible and avoid host-specific items. Currently the design has no hooks to reconfigure physical switches when deploying a new host. Any such requirement would need special handling.

To set up stateless deployment, one ESXi host must be installed in the standard fashion. Then find and record the following network-related information to save in the host profile:

- vSphere standard switch instances and settings (port groups, uplinks, MTU, and so forth)
- Distributed switch instances
- Selection rules for uplinks and uplink port or port groups
- vNIC information:
  - Address information (IPv4 or IPv6, static or DHCP, gateway)
  - Port groups and distributed port groups assigned to the physical network adapter (`vmknic`)
  - If there are distributed switches, record VLAN, physical NICs bound to the `vmknic`, and if `Etherchannel` is configured

The recorded information is used as a template for the host profile. Once the host profile virtual switch information has been extracted and placed in the host profile, you have the opportunity to change any of the information. Modifications are offered for both standard and distributed switches in these sections: uplink selection policy, based on either vmnic name or device number, and auto discovery based on VLAN ID. The (possibly modified) information is stored by the stateless boot infrastructure and applied to a stateless ESXi host on its next boot. During network initialization, a generic network plug-in interprets the recorded host profile setting and does the following:

- Loads appropriate physical NIC drivers.
- Creates all standard switch instances, along with port groups. It selects uplinks based on policy. If the policy is based on the VLAN ID, there is a probing process to gather relevant information.
- For VMkernel network adapters connected to the standard switch, it creates VMkernel network adapters and connects them to port groups.
- For each VMkernel network adapter connected to a distributed switch, it creates a temporary standard switch (as needed) with uplinks bound to the VMkernel network adapter. It creates a temporary port group with VLAN and teaming policies based on recorded information. Specifically, IP-hash is used if Etherchannel was used in the distributed switch.
- Configures all VMkernel network adapter settings (assigns address, gateway, MTU, and so forth).

Basic connectivity is functioning, and the networking setup is complete if there is no distributed switch present.

If there is a distributed switch present, the system stays in maintenance mode until distributed switch remediation is complete. No virtual machines are started at this time. Because distributed switches requires vCenter Server, the boot process continues until vCenter Server connectivity is established, and vCenter Server notices that the host should be part of a distributed switch. It issues a distributed switch host join, creating a distributed switch proxy standard switch on the host, selects appropriate uplinks, and migrates the vmknic from the standard switch to the distributed switch. When this operation is complete, it deletes the temporary standard switch and port groups.

At the end of the remediation process, the ESXi host is taken out of maintenance mode, and HA or DRS can start virtual machines on the host.

In the absence of a host profile, a temporary standard switch is created with “default networking” logic, which creates a management network switch (with no VLAN tag) whose uplink corresponds to the PXE booting vNIC. A vmknic is created on the management network port group with the same MAC address as the PXE booting vNIC. This logic was previously used for PXE booting. If there is a host profile, but the networking host profile is deactivated or fatally incomplete, vCenter Server falls back to default networking so that the ESXi host can be managed remotely. This triggers a compliance failure, so vCenter Server then initiates recovery actions.

Networking Best Practices

Consider these best practices when you configure your network.

- To ensure a stable connection between , , and other products and services, do not set connection limits and timeouts between the products. Setting limits and timeouts can affect the packet flow and cause services interruption.
- Isolate from one another the networks for host management, vSphere vMotion, vSphere FT, and so on, to improve security and performance.
- Dedicate a separate physical NIC to a group of virtual machines, or use Network I/O Control and traffic shaping to guarantee bandwidth to the virtual machines. This separation also enables distributing a portion of the total networking workload across multiple CPUs. The isolated virtual machines can then better handle application traffic, for example, from a vSphere Client.
- To physically separate network services and to dedicate a particular set of NICs to a specific network service, create a vSphere Standard Switch or vSphere Distributed Switch for each service. If this is not possible, separate network services on a single switch by attaching them to port groups with different VLAN IDs. In either case, verify with your network administrator that the networks or VLANs you choose are isolated from the rest of your environment and that no routers connect them.
- Keep the vSphere vMotion connection on a separate network. When migration with vMotion occurs, the contents of the guest operating system’s memory is transmitted over the network. You can do this either by using VLANs to segment a single physical network or by using separate physical networks (the latter is preferable).

  For migration across IP subnets and for using separate pools of buffer and sockets, place traffic for vMotion on the vMotion TCP/IP stack, and traffic for migration of powered-off virtual machines and cloning on the Provisioning TCP/IP stack. See VMkernel Networking Layer.
- Multihoming in VMkernel networking is not supported. For more information, see http://kb.vmware.com/kb/2010877.
- You can add and remove network adapters from a standard or distributed switch without affecting the virtual machines or the network service that is running behind that switch. If you remove all the running hardware, the virtual machines can still communicate among themselves. If you leave one network adapter intact, all the virtual machines can still connect with the physical network.
- To protect your most sensitive virtual machines, deploy firewalls in virtual machines that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks.
- For best performance, use VMXNET 3 virtual machine NICs.
- Physical network adapters connected to the same vSphere Standard Switch or vSphere Distributed Switch should also be connected to the same physical network.
- Configure the same MTU on all VMkernel network adapters in a vSphere Distributed Switch. If several VMkernel network adapters, configured with different MTUs, are connected to vSphere distributed switches, you might experience network connectivity problems.

Troubleshooting Networking

The troubleshooting topics about networking in vSphere provide solutions to potential problems that you might encounter with the connectivity of ESXi hosts, vCenter Server and virtual machines.

Guidelines for Troubleshooting

To troubleshoot your implementation of vSphere, identify the symptoms of the problem, determine which of the components are affected, and test possible solutions.

Identifying Symptoms	A number of potential causes might lead to the under-performance or nonperformance of your implementation. The first step in efficient troubleshooting is to identify exactly what is going wrong.
Defining the Problem Space	After you have isolated the symptoms of the problem, you must define the problem space. Identify the software or hardware components that are affected and might be causing the problem and those components that are not involved.
Testing Possible Solutions	When you know what the symptoms of the problem are and which components are involved, test the solutions systematically until the problem is resolved.

Identifying Symptoms

Before you attempt to resolve a problem in your implementation, you must identify precisely how it is failing.

The first step in the troubleshooting process is to gather information that defines the specific symptoms of what is happening. You might ask these questions when gathering this information:

- What is the task or expected behavior that is not occurring?
- Can the affected task be divided into subtasks that you can evaluate separately?
- Is the task ending in an error? Is an error message associated with it?
- Is the task completing but in an unacceptably long time?
- Is the failure consistent or sporadic?
- What has changed recently in the software or hardware that might be related to the failure?

Defining the Problem Space

After you identify the symptoms of the problem, determine which components in your setup are affected, which components might be causing the problem, and which components are not involved.

To define the problem space in an implementation of vSphere, be aware of the components present. In addition to VMware software, consider third-party software in use and which hardware is being used with the VMware virtual hardware.

Recognizing the characteristics of the software and hardware elements and how they can impact the problem, you can explore general problems that might be causing the symptoms.

- Misconfiguration of software settings
- Failure of physical hardware
- Incompatibility of components

Break down the process and consider each piece and the likelihood of its involvement separately. For example, a case that is related to a virtual disk on local storage is probably unrelated to third-party router configuration. However, a local disk controller setting might be contributing to the problem. If a component is unrelated to the specific symptoms, you can probably eliminate it as a candidate for solution testing.

Think about what changed in the configuration recently before the problems started. Look for what is common in the problem. If several problems started at the same time, you can probably trace all the problems to the same cause.

Testing Possible Solutions

After you know the problem's symptoms and which software or hardware components are most likely involved, you can systematically test solutions until you resolve the problem.

With the information that you have gained about the symptoms and affected components, you can design tests for pinpointing and resolving the problem. These tips might make this process more effective.

- Generate ideas for as many potential solutions as you can.
- Verify that each solution determines unequivocally whether the problem is fixed. Test each potential solution but move on promptly if the fix does not resolve the problem.
- Develop and pursue a hierarchy of potential solutions based on likelihood. Systematically eliminate each potential problem from the most likely to the least likely until the symptoms disappear.
- When testing potential solutions, change only one thing at a time. If your setup works after many things are changed at once, you might not be able to discern which of those things made a difference.
- If the changes that you made for a solution do not help resolve the problem, return the implementation to its previous status. If you do not return the implementation to its previous status, new errors might be introduced.
- Find a similar implementation that is working and test it in parallel with the implementation that is not working properly. Make changes on both systems at the same time until few differences or only one difference remains between them.

Troubleshooting with vCenter Server Logs

You can often obtain valuable troubleshooting information by looking at the logs provided by the various services and agents that your implementation is using.

Most logs are located in `/var/log/vmware/<service_name>` for vCenter Server deployments.

Common Logs

The following logs are common to all vCenter Server deployments.

Table 199: Common Log Directories

Log Directory	Description
`../firstboot`	Stores first boot logs
`applmgmt` and `applmgmt-audit`	Stores logs related to the VMware Appliance Management Service
`cloudvm`	Stores logs for allotment and distribution of resources between services
`rhttpproxy`	Stores logs for the VMware HTTP Reverse Proxy service
`sca`	Stores logs for the VMware Service Control Agent service
`vapi`	Stores logs for the VMware vAPI Endpoint service
`vmafdd`	Stores logs for the VMware Authentication Framework - LDAP service
`vmdird`	Stores logs for the VMware Directory Service - LDAP service
`vmon`	Stores logs for the VMware Service Lifecycle Manager service

Management Node Logs

The following logs are available if a management node deployment is selected.

Table 200: Management Node Log Directories

Log Directory	Service
`rbd`	VMware vSphere Auto Deploy
`content-library`	VMware Content Library Service
`eam`	VMware ESX Agent Manager
`netdumper`	VMware vSphere ESXi Dump Collector
`perfcharts`	VMware Performance Charts Service
`vmcam`	VMware vSphere Authentication Proxy
`vmdird`	VMware Directory Service - LDAP
`vmware-sps`	VMware vSphere Profile-Driven Storage Service
`vpxd`	VMware vCenter Server
`vpostgres`	VMware Postgres service
`vcha`	VMware vCenter High Availability service

Troubleshooting MAC Address Allocation

In vSphere, certain restrictions on the range of MAC addresses that can be assigned to virtual machines might cause lost of connectivity or inability to power on workloads.

Duplicate MAC Addresses of Virtual Machines on the Same Network

You encounter loss of packets and connectivity because virtual machines have duplicate MAC addresses generated by vCenter Server.

The MAC addresses of virtual machines on the same broadcast domain or IP subnet are in conflict, or vCenter Server generates a duplicate MAC address for a newly created virtual machine.

A virtual machine powers on and functions properly, but shares a MAC address with another virtual machine. This situation might cause packet loss and other problems.

Virtual machines might have duplicate MAC addresses due to several reasons.

- Two vCenter Server instances with identical IDs generate overlapping MAC addresses for virtual machine network adapters.
  Each vCenter Server instance has an ID between 0 and 63 that is randomly generated at installation time, but can be reconfigured after installation. vCenter Server uses the instance ID to generate MAC addresses for the network adapters of the machine.
- A virtual machine has been transferred in power-off state from one vCenter Server instance to another in the same network, for example, by using shared storage, and a new virtual machine network adapter on the first vCenter Server receives the freed MAC address.

- Change the MAC address of a virtual machine network adapter manually.

  If you have an existing virtual machine with a conflicting MAC address, you must provide a unique MAC address in the **Virtual Hardware** settings.

  - Power off the virtual machine, configure the adapter to use a manual MAC address, and type the new address.
  - If you cannot power the virtual machine off for configuration, re-create the network adapter that is in conflict with enabled manual MAC address assignment and type the new address. In the guest operating system, set the same static IP address to the re-added adapter as before.

  For information about configuring the network adapters of virtual machines, see the *vSphere Networking* and *vSphere Virtual Machine Administration* documentation.
- If the vCenter Server instance generates the MAC addresses of virtual machines according to the default allocation, VMware OUI, change the vCenter Server instance ID or use another allocation method to resolve conflicts.

  Note: Changing the vCenter Server instance ID or switching to a different allocation scheme does not resolve MAC address conflicts in existing virtual machines. Only virtual machines created or network adapters added after the change receive addresses according to the new scheme.

  For information about MAC address allocation schemes and setup, see the *vSphere Networking* documentation.

Solution	Description
Change the vCenter Server ID	You can keep using the VMware OUI allocation scheme if your deployment contains a small number of vCenter Server instances. According to this scheme, a MAC address has the following format: `00:50:56:XX:YY:ZZ` where `00:50:56` represents the VMware OUI, *XX* is calculated as (80 + vCenter Server ID), and *YY:ZZ* is a random number. To change the vCenter Server ID, configure the **vCenter Server unique ID** option in the **Runtime Settings** section from the **General** settings of the vCenter Server instance and restart it. The VMware OUI allocation works with up to 64 vCenter Server instances and is suitable for small scale deployments.
Switch to prefix-based allocation	You can use a custom OUI. For example, for a `02:12:34` locally administered address range, MAC addresses have the form `02:12:34:XX:YY:ZZ` . You can use the fourth octet *XX* to distribute the OUI address space between the vCenter Server instances. This structure results in 255 address clusters, each cluster managed by a vCenter Server instance, and in about 65000 MAC addresses per vCenter Server. For example, `02:12:34:01:YY:ZZ` for vCenter Server A, `02:12:34:02:YY:ZZ` for vCenter Server B, and so on. Prefix-based allocation is suitable for deployments of a larger scale.

Solution	Description
	For globally unique MAC addresses, the OUI must be registered in IEEE.

a) Configure MAC address allocation.
b) Apply the new MAC address allocation scheme to an existing virtual machine in its **Virtual Hardware** settings.
   - Power off a virtual machine, configure the adapter to use a manual MAC address, revert to automatic MAC address allocation, and power on the virtual machine.
   - If the virtual machine is in production and you cannot power it off for configuration, after you change the vCenter Server ID or the address allocation scheme, re-create the network adapter in conflict with enabled automatic MAC address assignment. In the guest operating system, set the same static IP address to the re-added adapter as before.

- Enforce MAC address regeneration when transferring a virtual machine between vCenter Server instances by using the virtual machine files from a datastore.
  a) Power off a virtual machine, remove it from the inventory, and in its configuration file (`.vmx`), set the `ethernetX.addressType` parameter to `generated`.
     `X` next to `ethernet` stands for the sequence number of the virtual NIC in the virtual machine.
  b) Import the virtual machine from one vCenter Server system to another by registering the virtual machine from a datastore in the target vCenter Server.
     The virtual machine files can reside in a datastore that is shared between the two vCenter Server instances or can be uploaded to a datastore that is accessible only from the target vCenter Server system.
     For information about registering a virtual machine from a datastore, see *vSphere Virtual Machine Administration*.
  c) Power on the virtual machines for the first time.
     While the virtual machine is starting up, an information icon appears on the virtual machine in the vSphere Client.
  d) Right-click the virtual machine and select **Guest OS** > **Answer Question**.
  e) Select the **I Copied It** option.

  The target vCenter Server re-generates the MAC address of the virtual machine. The new MAC address starts with the VMware OUI `00:0c:29` and is based on the BIOS UUID of the virtual machine. The BIOS UUID of the virtual machine is calculated from the BIOS UUID of the host.
- If the vCenter Server and hosts are version 6.0 and later and the vCenter Server instances are connected in Enhanced Linked Mode, migrate virtual machines by using vMotion across vCenter Server systems.
  When a virtual machine is migrated across vCenter Server systems, the source vCenter Server adds the MAC address of the virtual machine to a denylist and does not assign them to other virtual machines.

Attempt to Power On a Virtual Machine Fails Due to a MAC Address Conflict

After you set a certain static MAC address to a virtual machine adapter, you cannot power on the virtual machine.

In the vSphere Client, after you assign a MAC address within the range `00:50:56:40:`*`YY`*`:`*`ZZ`* – `00:50:56:7F:`*`YY`*`:`*`ZZ`* to a virtual machine, attempts to power the virtual machine on fail with a status message that the MAC address is in conflict.

```
00:50:56:XX:YY:ZZ is not a valid static Ethernet address. It
conflicts with VMware reserved MACs for other usage.
```

You attempt to assign a MAC address which starts with the VMware OUI `00:50:56` and is within the address range allocated for host VMkernel adapters on the vCenter Server system.

If you want to preserve the VMware OUI prefix, set a static MAC address within the range `00:50:56:00:00:00` – `00:50:56:3F:FF:FF` . Otherwise, set an arbitrary MAC address whose prefix is different from the VMware OUI one.

For information about the ranges available for static MAC addresses that have the VMware OUI prefix, see the *vSphere Networking* documentation.

Unable to Remove a Host from a vSphere Distributed Switch

Under certain conditions, you might be unable to remove a host from the vSphere distributed switch.

- Attempts to remove a host from a vSphere distributed switch fail, and you receive a notification that resources are still in use. The notification that you receive might look like the following:
  ```
  The resource '16' is in use.
  vDS DSwitch port 16 is still on host 10.23.112.2 connected to MyVM nic=4000 type=vmVnic
  ```
- Attempts to remove a host proxy switch that still exists on the host from a previous networking configuration fail. For example, you moved the host to a different data center or system, or upgraded the and software, and created new networking configuration. When trying to remove the host proxy switch, the operation fails because resources on the proxy switch are still in use.

You cannot remove the host from the distributed switch or delete the host proxy switch because of the following reasons.

- There are VMkernel adapters on the switch that are in use.
- There are virtual machine network adapters connected to the switch.

Problem	Solution
Cannot remove a host from a distributed switch	1. In the vSphere Client, navigate to the distributed switch. 2. On the **Configure** tab, select **More** > **Ports**. 3. Locate all ports that are still in use and check which VMkernel or virtual machine network adapters on the host are still attached to the ports. 4. Migrate or delete the VMkernel and virtual machine network adapters that are still connected to the switch. 5. Use the **Add and Manage Hosts** wizard in the vSphere Client to remove the host from the switch. After the host is removed, the host proxy switch is deleted automatically.
Cannot remove a host proxy switch	1. In the vSphere Client, navigate to the host. 2. Delete or migrate any VMkernel or virtual machine network adapters that are still connected to the host proxy switch. 3. Delete the host proxy switch from the Networking view on the host.

Hosts on a vSphere Distributed Switch Lose Connectivity to vCenter Server

Hosts on a vSphere Distributed Switch cannot connect to vCenter Server after a port group configuration.

After you change the networking configuration of a port group on a vSphere Distributed Switch that contains the VMkernel adapters for the management network, the hosts on the switch lose connectivity to vCenter Server. In the vSphere Client the status of the hosts is nonresponsive.

On a vSphere Distributed Switch in the vCenter Server that has networking rollback deactivated, the port group containing the VMkernel adapters for the management network is misconfigured in vCenter Server and the invalid configuration is propagated to the hosts on the switch.

Note: In vSphere networking rollback is enabled by default. However, you can activate or deactivate rollbacks at the vCenter Server level. For more information, see the *vSphere Networking* documentation.

1. From the Direct Console User Interface (DCUI) to an affected host, use the **Restore vDS** option from the **Network Restore Options** menu to configure the uplinks and the ID of the VLAN for the management network.

   The DCUI creates a local ephemeral port and applies the VLAN and uplink configuration to the port. The DCUI changes the VMkernel adapter for the management network to use the new host local port to restore connectivity to vCenter Server.

   After the host re-connects to vCenter Server, the vSphere Client displays a warning that some hosts on the switch have different networking configuration from the configuration stored in vSphere distributed switch.

2. In the vSphere Client, configure the distributed port group for the management network with correct settings.

Situation	Solution
You have altered the port group configuration only once	You can roll the configuration of the port group back one step. Right-click the port group, click **Restore Configuration**, and select **Restore to previous configuration**.
You have backed up a valid configuration of the port group	You can restore the configuration of the port group by using the backup file. Right-click the port group, click **Restore Configuration**, and select **Restore configuration from a file**. You can also restore the configuration for the entire switch, including the port group, from a backup file for the switch.
You have performed more than one configuration step and you do not have a backup file	You must provide valid settings for the port group manually.

   For information about networking rollback, recovery, and restore, see the *vSphere Networking* documentation.

3. Migrate the VMkernel adapter for the management network from the host local ephemeral port to a distributed port on the switch by using the **Add and Manage Hosts** wizard.

   Unlike distributed ports, the ephemeral local port of the VMKernel has a non-numeric ID.

   For information about handling VMkernel adapters through the **Add and Manage Hosts** wizard, see the *vSphere Networking* documentation.

4. Apply the configuration of the distributed port group and VMkernel adapter from vCenter Server to the host.
   - Push the correct configuration of the distributed port group and VMkernel adapter from vCenter Server to the host.
     a. In the vSphere Client, navigate to the host.
     b. On the **Configure** tab, click **Networking**.
     c. From the **Virtual switches** list, select the distributed switch and click **Rectify the state of the selected distributed switch on the host**.
   - Wait until vCenter Server applies the settings within the next 24 hours.

Alarm for Loss of Network Redundancy on a Host

An alarm reports a loss of uplink redundancy on a vSphere standard or a distributed switch for a host.

No redundant physical NICs for a host are connected to a particular standard or a distributed switch, and the following alarm appears:

```
Host name or IP Network uplink redundancy lost
```

Only one physical NIC on the host is connected to a certain standard or a distributed switch. The redundant physical NICs are either down or are not assigned to the switch.

For example, assume that a host in your environment has physical NICs *vmnic0* and *vmnic1* connected to *vSwitch0*, and the physical NIC *vmnic1* goes offline, leaving only *vmnic0* connected to *vSwitch0*. As a result, the uplink redundancy for *vSwitch0* is lost on the host.

Check which switch has lost uplink redundancy on the host. Connect at least one more physical NIC on the host to this switch and reset the alarm to green. You can use the vSphere Client or the ESXi Shell.

If a physical NIC is down, try to bring it back up by using the ESXi Shell on the host.

For information about using the networking commands in the ESXi Shell, see *ESXCLI Reference*. For information about configuring networking on a host in the vSphere Client, see *vSphere Networking*.

Virtual Machines Lose Connectivity After Changing the Uplink Failover Order of a Distributed Port Group

Changes in the failover NIC order on a distributed port group cause the virtual machines associated with the group to disconnect from the external network.

After you rearrange the uplinks in the failover groups for a distributed port group in vCenter Server, for example, by using the vSphere Client, some virtual machines in the port group can no longer access the external network.

After changing the failover order, many reasons might cause virtual machines to lose connectivity to the external network.

- The host that runs the virtual machines does not have physical NICs associated with the uplinks that are set to active or standby. All uplinks that are associated with physical NICs from the host for the port group are moved to unused.
- A Link Aggregation Group (LAG) that has no physical NICs from the host is set as the only active uplink according to the requirements for using LACP in vSphere.
- If the virtual machine traffic is separated in VLANs, the host physical adapters for the active uplinks might be connected to trunk ports on the physical switch that do not handle traffic from these VLANs.
- If the port group is configured with IP hash load balancing policy, an active uplink adapter is connected to a physical switch port that might not be in an EtherChannel.

You can examine the connectivity of the virtual machines in the port group to associated host uplinks and uplink adapters from the central topology diagram of the distributed switch or from the proxy switch diagram for the host.

- Restore the failover order with the uplink that is associated with a single physical NIC on the host back to active.
- Create a port group with identical settings, make it use the valid uplink number for the host, and migrate the virtual machine networking to the port group.
- Move the NIC to an uplink that participates in the active failover group.

  You can use the vSphere Client to move the host physical NIC to another uplink.

  - Use the **Add and Manage Hosts** wizard on the distributed switch.

    a. Navigate to the distributed switch in the vSphere Client.
    b. From the **Actions** menu select **Add and Manage Hosts**.
    c. On the **Select task** page, select the **Manage host networking** option and select the host.
    d. To assign the NIC of the host to an active uplink, navigate to the **Manage physical network adapters** page and associate the NIC to the switch uplink.
  - Move the NIC at the level of the host.

    a. Navigate to the host in the vSphere Client, and on the **Configure** tab, expand the **Networking** menu.
    b. Select **Virtual Switches** and select the distributed proxy switch.
    c. Click **Manage the physical network adapters connected to the selected switch**, and move the NIC to the active uplink

Unable to Add a Physical Adapter to a vDS That Has Network I/O Control

You might be unable to add a physical adapter with low speed, for example, 1 Gbps, to a vSphere Distributed Switch that has vSphere Network I/O Control version 3 configured.

You try to add a physical adapter with low speed, for example, 1 Gbps, to a vSphere Distributed Switch that is connected to physical adapters with high speed, for example, 10 Gbps. Network I/O Control version 3 is enabled on the switch and bandwidth reservations exist for one or more system traffic types, such as vSphere management traffic, vSphere vMotion traffic, vSphere NFS traffic, and so on. The task for adding the physical adapter fails with a status message that a parameter is incorrect.

```
A specified parameter was not correct: spec.host[].backing.pnicSpec[]
```

Network I/O Control aligns the bandwidth that is available for reservation to the 10-Gbps speed of the individual physical adapters that are already connected to the distributed switch. After you reserve a part of this bandwidth, adding a physical adapter whose speed is less than 10 Gbps might not meet the potential needs of a system traffic type.

For information about Network I/O Control version 3, see the *vSphere Networking* documentation.

1. In the , navigate to the host.
2. On the **Configure** tab, expand the **System** group of settings.
3. Select **Advanced System Settings** and click **Edit**.
4. Type the physical adapters that you want to use outside the scope of Network I/O Control as a comma-separated list for the `Net.IOControlPnicOptOut` parameter.
   For example: `vmnic2,vmnic3`
5. Click **OK** to apply the changes.
6. In the vSphere Client, add the physical adapter to the distributed switch.

Troubleshooting SR-IOV Enabled Workloads

Under certain conditions, you might experience connectivity or power-on problems with virtual machines that use SR-IOV to send data to physical network adapters.

SR-IOV Enabled Workload Cannot Communicate After You Change Its MAC Address

After you change the MAC address in the guest operating system of an SR-IOV enabled virtual machine, the virtual machine loses connectivity.

When you connect the network adapter of a virtual machine to an SR-IOV virtual function (VF), you create a passthrough network adapter for the virtual machine. After the (VF) driver in the guest operating system modifies the MAC address for the passthrough network adapter, the guest operating system shows that the change is successful but the VM network adapter loses connectivity. Although the guest operating system shows that the new MAC address is enabled, a log message in the `/var/log/vmkernel.log` file indicates that the operation has failed.

```
Requested mac address change to new MAC address on port VM NIC port number, disallowed by
 vswitch policy.
```

where

- *`new MAC address`* is the MAC address in the guest operation system.
- *`VM NIC port number`* is the port number of the VM network adapter in hexadecimal format.

The default security policy on the port group to which the passthrough network adapter is connected does not allow changes in the MAC address in the guest operating system. As a result, the networking interface in the guest operating system cannot acquire an IP address and loses connectivity.

In the guest operating system, reset the interface to cause the passthrough network adapter to regain its valid MAC address. If the interface is configured to use DHCP for address assignment, the interface acquires an IP address automatically.
For example, on a Linux virtual machine run the `ifconfig` console command.

```
ifconfig ethX down
ifconfig ethX up
```

where *X* in `ethX` represents the sequence number of the virtual machine network adapter in the guest operating system.

A Virtual Machine that Runs a VPN Client Causes Denial of Service for Virtual Machines on the Host or Across a vSphere HA Cluster

A virtual machine sending Bridge Protocol Data Unit (BPDU) frames, for example, a VPN client, causes some virtual machines connected to the same port group to lose connectivity. The transmission of BPDU frames might also break the connection of the host or of the parent vSphere HA cluster.

A virtual machine that is expected to send BPDU frames causes the traffic to the external network of the virtual machines in the same port group to be blocked.

If the virtual machine runs on a host that is a part of a vSphere HA cluster, and the host becomes network-isolated under certain conditions, you observe Denial of Service (DoS) on the hosts in the cluster.

As a best practice, a physical switch port that is connected to an ESXi host has the Port Fast and BPDU guard enabled to enforce the boundary of the Spanning Tree Protocol (STP). A standard or distributed switch does not support STP, and it does not send any BPDU frames to the switch port. However, if any BPDU frame from a compromised virtual machine arrives at a physical switch port facing an ESXi host , the BPDU guard feature disables the port to stop the frames from affecting the Spanning Tree Topology of the network.

In certain cases a virtual machine is expected to send BPDU frames, for example, when deploying VPN that is connected through a Windows bridge device or through a bridge function. If the physical switch port paired with the physical adapter that handles the traffic from this virtual machine has the BPDU guard on, the port is error-disabled, and the virtual machines and VMkernel adapters using the host physical adapter cannot communicate with the external network anymore.

If the teaming and failover policy of the port group contains more active uplinks, the BPDU traffic is moved to the adapter for the next active uplink. The new physical switch port becomes disabled, and more workloads become unable to exchange packets with the network. Eventually, almost all entities on the ESXi host might become unreachable.

If the virtual machine runs on a host that is a part of a vSphere HA cluster, and the host becomes network-isolated because most of the physical switch ports connected to it are disabled, the active primary host in the cluster moves the BPDU sender virtual machine to another host. The virtual machine starts disabling the physical switch ports connected to the new host. The migration across the vSphere HA cluster eventually leads to accumulated DoS across the entire cluster.

- If the VPN software must continue its work on the virtual machine, allow the traffic out of the virtual machine and configure the physical switch port individually to pass the BPDU frames.

Network Device	Configuration
Distributed or standard switch	Set the Forged Transmit security property on the port group to **Accept** to allow BPDU frames to leave the host and reach the physical switch port. You can isolate the settings and the physical adapter for the VPN traffic by placing the virtual machine in a separate port group and assigning the physical adapter to the group.

Network Device	Configuration
	CAUTION: Setting the Forged Transmit security property to **Accept** to enable a host to send BPDU frames carries a security risk because a compromised virtual machine can perform spoofing attacks.
Physical switch	• Keep the Port Fast enabled. • Enable the BPDU filter on the individual port. When a BPDU frame arrives at the port, it is filtered out. **Note:** Do not enable the BPDU filter globally. If the BPDU filter is enabled globally, the Port Fast mode becomes disabled and all physical switch ports perform the full set of STP functions.

- To deploy a bridge device between two virtual machine NICs connected to the same Layer 2 network, allow the BPDU traffic out of the virtual machines and deactivate Port Fast and BPDU loop prevention features.

Network Device	Configuration
Distributed or standard switch	Set the Forged Transmit property of the security policy on the port groups to **Accept** to allow BPDU frames to leave the host and reach the physical switch port. You can isolate the settings and one or more physical adapters for the bridge traffic by placing the virtual machine in a separate port group and assigning the physical adapters to the group. **CAUTION:** Setting the Forged Transmit security property to **Accept** to enable bridge deployment carries a security risk because a compromised virtual machine can perform spoofing attacks.
Physical switch	• Disable Port Fast on the ports to the virtual bridge device to run STP on them. • Disable BPDU guard and filter on the ports facing the bridge device.

- Protect the environment from DoS attacks in any case by activating the BPDU filter on the ESXi host or on the physical switch.
  - On a host that does not have the Guest BPDU filter implemented enable the BPDU filter on the physical switch port to the virtual bridge device.

Network Device	Configuration
Distributed or standard switch	Set the Forged Transmit property of the security policy on the port group to **Reject**.
Physical switch	• Keep the Port Fast configuration. • Enable the BPDU filter on the individual physical switch port. When a BPDU frame arrives at the physical port, it is filtered out. **Note:** Do not enable the BPDU filter globally. If the BPDU filter is enabled globally, the Port Fast mode becomes disabled and all physical switch ports perform the full set of STP functions.

Low Throughput for UDP Workloads on Windows Virtual Machines

When a Windows virtual machine in vSphere transmits large UDP packets, the throughput is lower than expected or is oscillating even when other traffic is negligible.

When a Windows virtual machine transmits UDP packets larger than 1024 bytes, you experience lower than expected or oscillating throughput even when other traffic is negligible. In case of a video streaming server, video playback pauses.

For every UDP packet larger than 1024 bytes, the Windows network stack waits for a transmit completion interrupt before sending the next packet. vSphere does not provide a transparent workaround of the situation.

- Increase the threshold in bytes at which Windows changes its behavior for UDP packets by modifying the registry of the Windows guest OS.
  a) Locate the `HKLM\System\CurrentControlSet\Services\Afd\Parameters` registry key.
  b) Add a value with the name `FastSendDatagramThreshold` of type DWORD equal to 1500.

  For information about fixing this issue in the Windows registry, see http://support.microsoft.com/kb/235257.
- Modify the coalescing settings of the virtual machine NIC.

  If the Windows virtual machine has a VMXNET3 vNIC adapter, configure one of the following parameters in the `.vmx` file of the virtual machine. Use the vSphere Client, or directly modify the `.vmx` file.

Action	Parameter	Value
Increase the interrupt rate of the virtual machine to a higher rate than expected packet rate. For example, if the expected packet rate is 15000 interrupts per second, set the interrupt rate to 16000 interrupts per second. Set the `ethernetX.coalescingScheme` parameter to `rbc` and the `ethernetX.coalescingParams` parameter to `16000`. The default interrupt rate is 4000 interrupts per second.	`ethernetX.coalescingScheme` `ethernetX.coalescingParams`	rbc 16000
Deactivate coalescing for low throughput or latency-sensitive workloads. For information about configuring low-latency workloads, see Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs.	`ethernetX.coalescingScheme`	disabled
Revert to the coalescing algorithm from earlier ESXi releases. **Note:** The ability to revert to the earlier algorithm will not be available in later vSphere releases.	`ethernetX.coalescingScheme`	calibrate

  X next to `ethernet` stands for the sequence number of the vNIC in the virtual machine.

  For more information about configuring parameters in the `.vmx` file, see the *vSphere Virtual Machine Administration*documentation.
- Modify ESXi host coalescing settings.

  This approach affects all virtual machines and all virtual machine NICs on the host.

  You can edit the advanced system settings list for the host in the vSphere Client, or by using a vCLI console command on the host from the ESXi Shell.

Action	Parameter in the vSphere Client	Parameter for the `esxcli system settings sdvanced set` Command	Value
Set a default interrupt rate higher than the expected packet rate. For example, set the interrupt rate to 16000 if 15000 interrupts are expected per second.	`Net.CoalesceScheme` `Net.CoalesceParams`	`/Net/CoalesceScheme` `/Net/CoalesceParams`	rbc 16000
Deactivate coalescing for low throughput or latency-sensitive workloads. For information about configuring low-latency workloads, see Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs.	`Net.CoalesceDefaultOn`	`/Net/CoalesceDefaultOn`	0
Revert to the coalescing scheme from earlier ESXi releases. **Note:** The ability to revert to the earlier algorithm will not be available in later vSphere releases.	`Net.CoalesceScheme`	`/Net/CoalesceScheme`	calibrate

For information about configuring a host from the vSphere Client, see the *vCenter Server and Host Management* documentation. For information about setting host properties by using a vCLI command, refer to the *ESXCLI Reference* documentation.

VMs on the Same Distributed Port Group are Unable to Communicate

Under certain conditions, the virtual machines that are on the same distributed port group but on different hosts cannot communicate with each other.

Virtual machines that reside on different hosts and on the same port group are unable to communicate. Pings from one virtual machine to another have no effect. You cannot migrate the virtual machines between the hosts by using vMotion.

- There are no physical NICs on some of the hosts assigned to active or standby uplinks in the teaming and failover order of the distributed port group.
- The physical NICs on the hosts that are assigned to the active or standby uplinks reside in different VLANs on the physical switch. The physical NICs in different VLANs cannot see each other and thus cannot communicate with each other.
- In the topology of the distributed switch, check which host does not have physical NICs assigned to an active or standby uplink on the distributed port group. Assign at least one physical NIC on that host to an active uplink on the port group.
- In the topology of the distributed switch, check the VLAN IDs of the physical NICs that are assigned to the active uplinks on the distributed port group. On all hosts, assign physical NICs that are from the same VLAN to an active uplink on the distributed port group.
- To verify that there is no problem at the physical layer, migrate the virtual machines to the same host and check the communication between them. Verify that inbound and outbound ICMP traffic is enabled in the guest OS. By default ICMP traffic is deactivated in Windows Server 2008 and Windows Server 2012.

Attempt to Power On a Migrated vApp Fails Because the Associated Protocol Profile Is Missing

You cannot power on a vApp or virtual machine that you transferred to a data center or a vCenter Server system because a network protocol profile is missing.

After you cold migrate a vApp or a virtual machine to another data center or vCenter Server system, an attempt to power it on fails. An error message states that a property cannot be initialized or allocated because the network of the vApp or virtual machine does not have an associated network protocol profile.

```
Cannot initialize property 'property'. Network 'port group' has no associated network
 protocol profile.
```

```
Cannot allocate IP address for property 'property'. Network 'port group' has no associated
 network protocol profile.
```

By using the OVF environment, the vApp or virtual machine retrieves network settings from a network protocol profile that is associated with the port group of the vApp or virtual machine.

vCenter Server creates such a network protocol profile for you when you install the OVF of a vApp and associates the profile with the port group that you specify during the installation.

The mapping between the protocol profile and port group is valid only in the scope of a data center. When you move the vApp, the protocol profile is not transferred to the target data center because of the following reasons:

- The network settings of the protocol profile might not be valid in the network environment of the target data center.
- A port group that has the same name and is associated with another protocol profile might already exist in the target data center, and vApps and virtual machines might be connected to this group. Replacing the protocol profiles for the port group might affect the connectivity of these vApp and virtual machines.

- Create a network protocol profile on the target data center or vCenter Server system with the required network settings and associate the protocol profile with the port group to which the vApp or virtual machine is connected. For example, this approach is suitable if the vApp or virtual machine is a vCenter Server extension that uses the vCenter Extension vService.

  For information about providing network settings to a vApp or virtual machine from a network protocol profile, see the *vSphere Networking* documentation.
- Use the vSphere Client to export the OVF file of the vApp or virtual machine from the source data center or vCenter Server system and deploy it on the target data center or vCenter Server system.

  When you use the vSphere Client to deploy the OVF file, the target vCenter Server system creates the network protocol profile for the vApp.

  For information about managing OVF files in the vSphere Client, see the *vSphere Virtual Machine Administration* documentation.

Networking Configuration Operation Is Rolled Back and a Host Is Disconnected from vCenter Server

When you attempt to add or configure networking on a vSphere Distributed Switch on a host, the operation is rolled back and the host is disconnected from vCenter Server.

An attempt to perform a networking configuration operation on a vSphere Distributed Switch on a host, such as creating a virtual machine adapter or a port group, causes the host to disconnect from vCenter Server and results in the error message `Transaction has rolled back on the host`.

Under stressful conditions on a host, that is, if many concurrent networking operations compete for limited resources, the time to perform some of the operations might exceed the default timeout for rollback of network configuration operations on the distributed switch. As a result, these operations are rolled back.

For example, such a condition might come up when you create a VMkernel adapter on a host that has a very high number of switch ports or virtual adapters, all of which consume system resources on the host.

The default timeout to roll an operation back is 30 seconds.

- Use the vSphere Client to increase the timeout for rollback on vCenter Server.

  If you encounter the same problem again, increase the rollback timeout with 60 seconds incrementally until the operation has enough time to succeed.

  a) On the **Configure** tab of a vCenter Server instance, expand **Settings**.
  b) Select **Advanced Settings** and click **Edit**.
  c) If the property is not present, add the `config.vpxd.network.rollbackTimeout` parameter to the settings.
  d) Type a new value, in seconds, for the `config.vpxd.network.rollbackTimeout` parameter
  e) Click **OK**.
  f) Restart the vCenter Server system to apply the changes.
- Increase the timeout for rollback by editing the `vpxd.cfg` configuration file.

  If you encounter the same problem again, increase the rollback timeout with 60 seconds incrementally until the operation has enough time to succeed.

  a) On the host machine of , navigate to the directory `/etc/vmware-vpx`.
  b) Open the `vpxd.cfg` file for editing.
  c) Under the `<network>` section, increase the timeout, in the `<rollbackTimeout>` element.

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

  d) Save and close the file.
  e) Restart the vCenter Server system to apply the changes.

vSphere Storage

vSphere Storage describes virtualized and software-defined storage technologies that VMware ESXi™ and VMware vCenter Server® offer, and explains how to configure and use these technologies.

Intended Audience

This information is for experienced system administrators who are familiar with the virtual machine and storage virtualization technologies, data center operations, and SAN storage concepts.

Updated Information

This *vSphere Storage* is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Storage*.

Revision	Description
30 JUL 2024	Minor revisions.
28 SEP 2023	• Added the Migrating Container Volumes in vSphere topic. • Added a statement about amount of available space in the datastore for a core dump file. See Set Up a File as Core Dump Location. • Added a statement about tag-based rules at a datastore cluster level to Create a VM Storage Policy for Tag-Based Placement.
31 JUL 2023	Minor revisions.
29 JUN 2023	Updated statements about the SCSI `TimeoutValue` parameter in ESXi Fibre Channel SAN Requirements and ESXi iSCSI SAN Recommendations and Restrictions.
06 APR 2023	Clarified information about the latency mechanism that can be activated for the Round Robin path selection policy: • Path Selection Plug-Ins and Policies • Change Default Parameters for Latency Round Robin
13 FEB 2023	Updated Failures When Migrating VMs or Deploying VM OVFs to Virtual Volumes Datastores with a note that starting with vSphere 7.0 Update 2, partners can increase the config-vVol to 4 GB and more.
07 FEB 2023	Updated Set Up Dynamic Disk Mirroring.
06 FEB 2023	Updated HPP Best Practices to include recommendation to use VMware Paravirtual or NVMe controllers with VM. See VMware High Performance Plug-In and Path Selection Schemes.
02 FEB 2023	Minor revisions.
31 JAN 2023	Clarified information about replication groups in the following topics: • Virtual Volumes and Replication Groups • Virtual Volumes and Fault Domains
11 JAN 2023	Added privileges required when a VM is encrypted. See Download Files from Datastores.

Revision	Description
04 JAN 2023	Added a note with information about the `snapshot.alwaysAllowNative` parameter to Enable NAS Native Snapshots on Virtual Machines.
29 NOV 2022	Removed vSAN stretched cluster limitations from Requirements of Cloud Native Storage and Create a Storage Policy for Kubernetes.
28 OCT 2022	• Updated graphic in Example of Network Topology with NVMe over TCP. • Minor updates in Change Space Reclamation Settings.
24 AUG 2022	Minor revisions.
16 AUG 2022	Added a requirement to remount a datastore to Change Space Reclamation Settings.
29 JUL 2022	Clarified a replication group requirement for Virtual Volumes storage policy in Change Storage Policy Assignment for Virtual Machine Files and Disks.
26 JUL 2022	Minor revisions.
28 APR 2022	Minor revisions.
14 DEC 2021	Minor updates.
29 NOV 2021	Removed the following statement from VMware High Performance Plug-In and Path Selection Schemes: "Do not activate the HPP for HDDs or slower flash devices. The HPP is not expected to provide any performance benefits with devices incapable of at least 200 000 IOPS."
17 NOV 2021	Minor updates.
29 OCT 2021	Minor updates.
21 OCT 2021	Updated Configuring Network Access to vSAN File Share to indicate that using a dedicated vNIC for the file traffic is not mandatory.
05 OCT 2021	Initial release.

Introduction to Storage

vSphere supports various storage options and functionalities in traditional and software-defined storage environments. A high-level overview of vSphere storage elements and aspects helps you plan a proper storage strategy for your virtual data center.

Traditional Storage Virtualization Models

Generally, storage virtualization refers to a logical abstraction of physical storage resources and capacities from virtual machines and their applications. ESXi provides host-level storage virtualization.

In vSphere environment, a traditional model is built around the following storage technologies and ESXi and vCenter Server virtualization functionalities.

Local and Networked Storage

In traditional storage environments, the storage management process starts with storage space that your storage administrator preallocates on different storage systems.

ESXi

supports local storage and networked storage.

See Types of Physical Storage.

Storage Area Networks	A storage area network (SAN) is a specialized high-speed network that connects computer systems, or ESXi hosts, to high-performance storage systems. ESXi can use Fibre Channel or iSCSI protocols to connect to storage systems. See Overview of Using ESXi with a SAN.
Fibre Channel	Fibre Channel (FC) is a storage protocol that the SAN uses to transfer data traffic from ESXi host servers to shared storage. The protocol packages SCSI commands into FC frames. To connect to the FC SAN, your host uses Fibre Channel host bus adapters (HBAs). See Using ESXi with Fibre Channel SAN.
Internet SCSI	Internet iSCSI (iSCSI) is a SAN transport that can use Ethernet connections between computer systems, or ESXi hosts, and high-performance storage systems. To connect to the storage systems, your hosts use hardware iSCSI adapters or software iSCSI initiators with standard network adapters. See Using ESXi with iSCSI SAN.
Storage Device or LUN	In the ESXi context, the terms device and LUN are used interchangeably. Typically, both terms mean a storage volume that is presented to the host from a block storage system and is available for formatting. See Target and Device Representations and Managing Storage Devices.
Virtual Disks	A virtual machine on an ESXi host uses a virtual disk to store its operating system, application files, and other data associated with its activities. Virtual disks are large physical files, or sets of files, that can be copied, moved, archived, and backed up as any other files. You can configure virtual machines with multiple virtual disks. To access virtual disks, a virtual machine uses virtual SCSI controllers. These virtual controllers include BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual. These controllers are the only types of SCSI controllers that a virtual machine can see and access. Each virtual disk resides on a datastore that is deployed on physical storage. From the standpoint of the virtual machine, each virtual disk appears as if it were a SCSI drive connected to a SCSI controller. Whether the physical storage is accessed through storage or network adapters on the host is typically transparent to the VM guest operating system and applications.
VMware vSphere® VMFS	The datastores that you deploy on block storage devices use the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing virtual machines. See Understanding VMFS Datastores.
NFS	An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access an NFS volume that is located on a NAS server. The ESXi host can mount the volume and use it as an NFS datastore. See Understanding Network File System Datastores.
Raw Device Mapping	In addition to virtual disks, vSphere offers a mechanism called raw device mapping (RDM). RDM is useful when a guest operating

system inside a virtual machine requires direct access to a storage device. For information about RDMs, see Raw Device Mapping.

Software-Defined Storage Models

In addition to abstracting underlying storage capacities from VMs, as traditional storage models do, software-defined storage abstracts storage capabilities.

With the software-defined storage model, a virtual machine becomes a unit of storage provisioning and can be managed through a flexible policy-based mechanism. The model involves the following vSphere technologies.

VMware vSphere®Virtual Volumes™ (vVols)	The Virtual Volumes functionality changes the storage management paradigm from managing space inside datastores to managing abstract storage objects handled by storage arrays. With Virtual Volumes, an individual virtual machine, not the datastore, becomes a unit of storage management. And storage hardware gains complete control over virtual disk content, layout, and management. See Working with VMware vSphere Virtual Volumes.
VMware vSAN	vSAN is a distributed layer of software that runs natively as a part of the hypervisor. vSAN aggregates local or direct-attached capacity devices of an ESXi host cluster and creates a single storage pool shared across all hosts in the vSAN cluster. See *Administering VMware vSAN*.
Storage Policy Based Management	Storage Policy Based Management (SPBM) is a framework that provides a single control panel across various data services and storage solutions, including vSAN and Virtual Volumes. Using storage policies, the framework aligns application demands of your virtual machines with capabilities provided by storage entities. See Storage Policy Based Management.
I/O Filters	I/O filters are software components that can be installed on ESXi hosts and can offer additional data services to virtual machines. Depending on implementation, the services might include replication, encryption, caching, and so on. See Filtering Virtual Machine I/O.

vSphere Storage APIs

Storage APIs is a family of APIs used by third-party hardware, software, and storage providers to develop components that enhance several vSphere features and solutions.

This Storage publication describes several Storage APIs that contribute to your storage environment. For information about other APIs from this family, including vSphere APIs - Data Protection, see the VMware website.

vSphere APIs for Storage Awareness

Also known as VASA, these APIs, either supplied by third-party vendors or offered by VMware, enable communications between vCenter Server and underlying storage. Through VASA, storage entities can inform vCenter Server about their configurations, capabilities, and storage health and events. In return, VASA can deliver VM storage requirements from vCenter Server to a storage entity and ensure that the storage layer meets the requirements.

VASA becomes essential when you work with Virtual Volumes, vSAN, vSphere APIs for I/O Filtering (VAIO), and storage VM policies. See Using Storage Providers.

vSphere APIs for Array Integration

These APIs, also known as VAAI, include the following components:

- Hardware Acceleration APIs. Help arrays to integrate with vSphere, so that vSphere can offload certain storage operations to the array. This integration significantly reduces CPU overhead on the host. See Storage Hardware Acceleration.
- Array Thin Provisioning APIs. Help to monitor space use on thin-provisioned storage arrays to prevent out-of-space conditions, and to perform space reclamation. See ESXi and Array Thin Provisioning.

vSphere APIs for Multipathing

Known as the Pluggable Storage Architecture (PSA), these APIs allow storage partners to create and deliver multipathing and load-balancing plug-ins that are optimized for each array. Plug-ins communicate with storage arrays and determine the best path selection strategy to increase I/O performance and reliability from the ESXi host to the storage array. For more information, see Pluggable Storage Architecture and Path Management.

Getting Started with a Traditional Storage Model

Setting up your ESXi storage in traditional environments, includes configuring your storage systems and devices, enabling storage adapters, and creating datastores.

Types of Physical Storage

In traditional storage environments, the ESXi storage management process starts with storage space that your storage administrator preallocates on different storage systems. ESXi supports local storage and networked storage.

Local Storage

Local storage can be internal hard disks located inside your ESXi host. It can also include external storage systems located outside and connected to the host directly through protocols such as SAS or SATA.

Local storage does not require a storage network to communicate with your host. You need a cable connected to the storage unit and, when required, a compatible HBA in your host.

The following illustration depicts a virtual machine using local SCSI storage.

Figure 61: Local Storage

In this example of a local storage topology, the ESXi host uses a single connection to a storage device. On that device, you can create a VMFS datastore, which you use to store virtual machine disk files.

Although this storage configuration is possible, it is not a best practice. Using single connections between storage devices and hosts creates single points of failure (SPOF) that can cause interruptions when a connection becomes unreliable or fails. However, because most of local storage devices do not support multiple connections, you cannot use multiple paths to access local storage.

ESXi supports various local storage devices, including SCSI, IDE, SATA, USB, SAS, flash, and NVMe devices.

Note: You cannot use IDE/ATA or USB drives to store virtual machines.

Local storage does not support sharing across multiple hosts. Only one host has access to a datastore on a local storage device. As a result, although you can use local storage to create VMs, you cannot use VMware features that require shared storage, such as HA and vMotion.

However, if you use a cluster of hosts that have just local storage devices, you can implement vSAN. vSAN transforms local storage resources into software-defined shared storage. With vSAN, you can use features that require shared storage. For details, see the *Administering VMware vSAN* documentation.

Networked Storage

Networked storage consists of external storage systems that your ESXi host uses to store virtual machine files remotely. Typically, the host accesses these systems over a high-speed storage network.

Networked storage devices are shared. Datastores on networked storage devices can be accessed by multiple hosts concurrently. ESXi supports multiple networked storage technologies.

In addition to traditional networked storage that this topic covers, VMware supports virtualized shared storage, such as vSAN. vSAN transforms internal storage resources of your ESXi hosts into shared storage that provides such capabilities as High Availability and vMotion for virtual machines. For details, see the *Administering VMware vSAN* documentation.

Note: The same LUN cannot be presented to an ESXi host or multiple hosts through different storage protocols. To access the LUN, hosts must always use a single protocol, for example, either Fibre Channel only or iSCSI only.

Fibre Channel (FC)

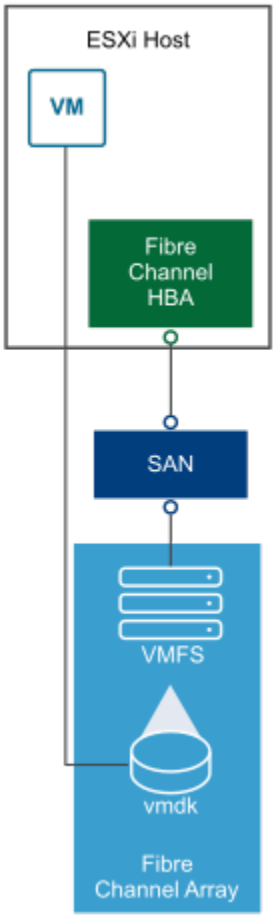
Stores virtual machine files remotely on an FC storage area network (SAN). FC SAN is a specialized high-speed network that connects your hosts to high-performance storage devices. The network uses Fibre Channel protocol to transport SCSI traffic from virtual machines to the FC SAN devices.

To connect to the FC SAN, your host should be equipped with Fibre Channel host bus adapters (HBAs). Unless you use Fibre Channel direct connect storage, you need Fibre Channel switches to route storage traffic. If your host contains FCoE (Fibre Channel over Ethernet) adapters, you can connect to your shared Fibre Channel devices by using an Ethernet network.

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

Fibre Channel Storage depicts virtual machines using Fibre Channel storage.

Figure 62: Fibre Channel Storage



In this configuration, a host connects to a SAN fabric, which consists of Fibre Channel switches and storage arrays, using a Fibre Channel adapter. LUNs from a storage array become available to the host. You can access the LUNs and create datastores for your storage needs. The datastores use the VMFS format.

For specific information on setting up the Fibre Channel SAN, see Using ESXi with Fibre Channel SAN.

Internet SCSI (iSCSI)

Stores virtual machine files on remote iSCSI storage devices. iSCSI packages SCSI storage traffic into the TCP/IP protocol, so that it can travel through standard TCP/IP networks instead of the specialized FC network. With an iSCSI connection, your host serves as the initiator that communicates with a target, located in remote iSCSI storage systems.

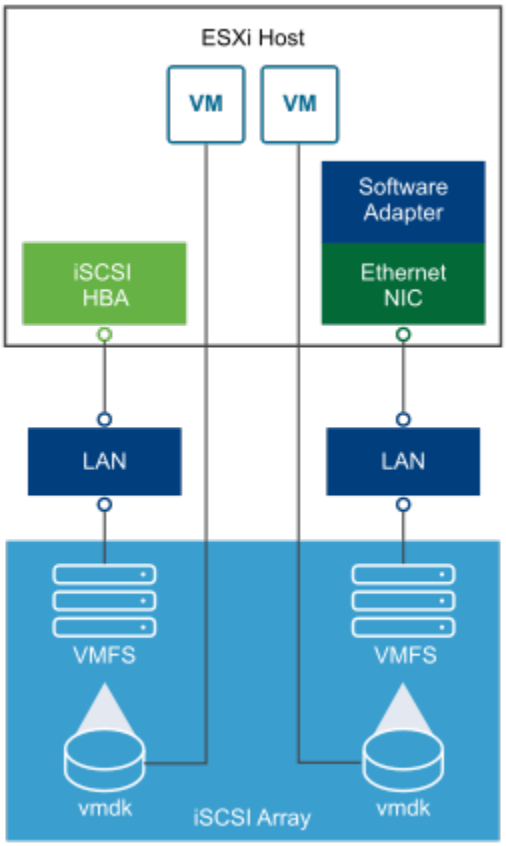
ESXi offers the following types of iSCSI connections:

Hardware iSCSI	Your host connects to storage through a third-party adapter capable of offloading the iSCSI and network processing. Hardware adapters can be dependent and independent.
Software iSCSI	Your host uses a software-based iSCSI initiator in the VMkernel to connect to storage. With this type of iSCSI connection, your host needs only a standard network adapter for network connectivity.

You must configure iSCSI initiators for the host to access and display iSCSI storage devices.

iSCSI Storage depicts different types of iSCSI initiators.

Figure 63: iSCSI Storage



In the left example, the host uses the hardware iSCSI adapter to connect to the iSCSI storage system.

In the right example, the host uses a software iSCSI adapter and an Ethernet NIC to connect to the iSCSI storage.

iSCSI storage devices from the storage system become available to the host. You can access the storage devices and create VMFS datastores for your storage needs.

For specific information on setting up the iSCSI SAN, see Using ESXi with iSCSI SAN.

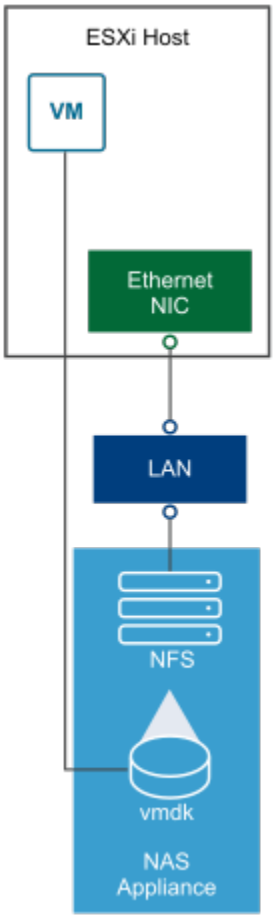
Network-attached Storage (NAS)

Stores virtual machine files on remote file servers accessed over a standard TCP/IP network. The NFS client built into ESXi uses Network File System (NFS) protocol version 3 and 4.1 to communicate with the NAS/NFS servers. For network connectivity, the host requires a standard network adapter.

You can mount an NFS volume directly on the ESXi host. You then use the NFS datastore to store and manage virtual machines in the same way that you use the VMFS datastores.

NFS Storage depicts a virtual machine using the NFS datastore to store its files. In this configuration, the host connects to the NAS server, which stores the virtual disk files, through a regular network adapter.

Figure 64: NFS Storage



For specific information on setting up NFS storage, see Understanding Network File System Datastores.

Shared Serial Attached SCSI (SAS)

Stores virtual machines on direct-attached SAS storage systems that offer shared access to multiple hosts. This type of access permits multiple hosts to access the same VMFS datastore on a LUN.

NVMe over Fabrics Storage

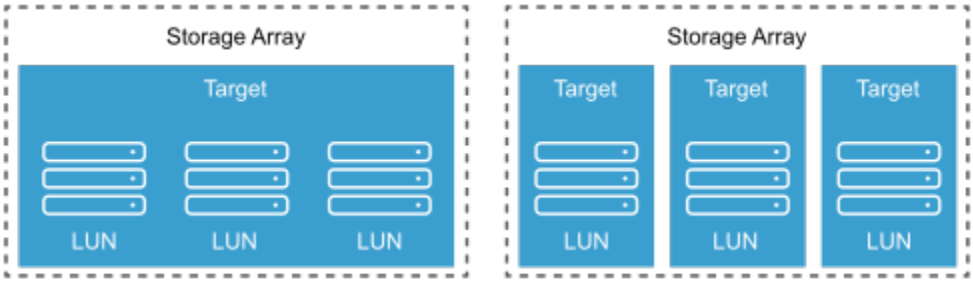
VMware NVMe over Fabrics (NVMe-oF) provides a distance connectivity between a host and a target storage device on a shared storage array. VMware supports NVMe over RDMA (with RoCE v2 technology), NVMe over Fibre Channel (FC-NVMe) transports, and NVMe over TCP/IP technology. For more information, see About VMware NVMe Storage.

Target and Device Representations

In the ESXi context, the term target identifies a single storage unit that the host can access. The terms storage device and LUN describe a logical volume that represents storage space on a target. In the ESXi context, both terms also mean a storage volume that is presented to the host from a storage target and is available for formatting. Storage device and LUN are often used interchangeably.

Different storage vendors present the storage systems to ESXi hosts in different ways. Some vendors present a single target with multiple storage devices or LUNs on it, while others present multiple targets with one LUN each.

Figure 65: Target and LUN Representations



In this illustration, three LUNs are available in each configuration. In one case, the host connects to one target, but that target has three LUNs that can be used. Each LUN represents an individual storage volume. In the other example, the host detects three different targets, each having one LUN.

Targets that are accessed through the network have unique names that are provided by the storage systems. The iSCSI targets use iSCSI names. Fibre Channel targets use World Wide Names (WWNs).

Note: ESXi does not support accessing the same LUN through different transport protocols, such as iSCSI and Fibre Channel.

A device, or LUN, is identified by its UUID name. If a LUN is shared by multiple hosts, it must be presented to all hosts with the same UUID.

How Virtual Machines Access Storage

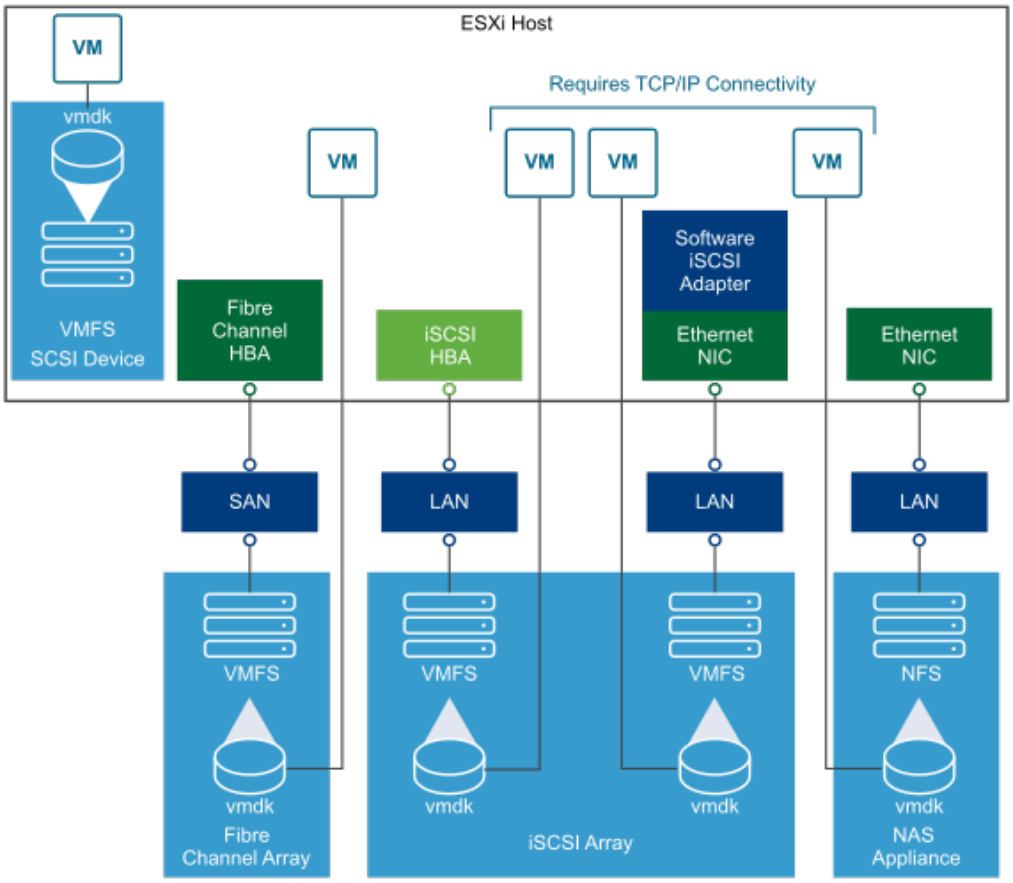
When a virtual machine communicates with its virtual disk stored on a datastore, it issues SCSI commands. Because datastores can exist on various types of physical storage, these commands are encapsulated into other forms, depending on the protocol that the ESXi host uses to connect to a storage device.

ESXi supports Fibre Channel (FC), Internet SCSI (iSCSI), Fibre Channel over Ethernet (FCoE), and NFS protocols. Regardless of the type of storage device your host uses, the virtual disk always appears to the virtual machine as a mounted SCSI device. The virtual disk hides a physical storage layer from the virtual machine's operating system. This allows you to run operating systems that are not certified for specific storage equipment, such as SAN, inside the virtual machine.

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

The following graphic depicts five virtual machines using different types of storage to illustrate the differences between each type.

Figure 66: Virtual machines accessing different types of storage



Note: This diagram is for conceptual purposes only. It is not a recommended configuration.

Storage Device Characteristics

When your ESXi host connects to block-based storage systems, LUNs or storage devices that support ESXi become available to the host.

After the devices get registered with your host, you can display all available local and networked devices and review their information. If you use third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

Note: If an array supports implicit asymmetric logical unit access (ALUA) and has only standby paths, the registration of the device fails. The device can register with the host after the target activates a standby path and the host detects it as active. The advanced system `/Disk/FailDiskRegistration` parameter controls this behavior of the host.

For each storage adapter, you can display a separate list of storage devices available for this adapter.

Generally, when you review storage devices, you see the following information.

Table 201: Storage Device Information

Storage Device Information	Description
Name	Also called Display Name. It is a name that the ESXi host assigns to the device based on the storage type and manufacturer. Generally, you can change this name to a name of your choice. See Rename Storage Devices.
Identifier	A universally unique identifier that is intrinsic to the device. See Storage Device Names and Identifiers.
Operational State	Indicates whether the device is attached or detached. See Detach Storage Devices.
LUN	Logical Unit Number (LUN) within the SCSI target. The LUN number is provided by the storage system. If a target has only one LUN, the LUN number is always zero (0).
Type	Type of device, for example, disk or CD-ROM.
Drive Type	Information about whether the device is a flash drive or a regular HDD drive. For information about flash drives and NVMe devices, see Working with Flash Devices.
Transport	Transportation protocol your host uses to access the device. The protocol depends on the type of storage being used. See Types of Physical Storage.
Capacity	Total capacity of the storage device.
Owner	The plug-in, such as the NMP or a third-party plug-in, that the host uses to manage paths to the storage device. See Pluggable Storage Architecture and Path Management.
Hardware Acceleration	Information about whether the storage device assists the host with virtual machine management operations. The status can be Supported, Not Supported, or Unknown. See Storage Hardware Acceleration.
Sector Format	Indicates whether the device uses a traditional, 512n, or advanced sector format, such as 512e or 4Kn. See Device Sector Formats.
Location	A path to the storage device in the `/vmfs/devices/` directory.
Partition Format	A partition scheme used by the storage device. It can be of a master boot record (MBR) or GUID partition table (GPT) format. The GPT devices can support datastores greater than 2 TB. See Device Sector Formats.
Partitions	Primary and logical partitions, including a VMFS datastore, if configured.
Multipathing Policies	Path Selection Policy and Storage Array Type Policy the host uses to manage paths to storage. See Understanding Multipathing and Failover.
Paths	Paths used to access storage and their status. See Disable Storage Paths.

Display Storage Devices for an ESXi Host

Display all storage devices available to a ESXi host. If you use any third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

The Storage Devices view allows you to list the hosts' storage devices, analyze their information, and modify properties.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
   All storage devices available to the host are listed in the Storage Devices table.

4. To view details for a specific device, select the device from the list.
5. Use the icons to perform basic storage management tasks.

   Availability of specific icons depends on the device type and configuration.

Icon	Description
Refresh	Refresh information about storage adapters, topology, and file systems.
Detach	Detach the selected device from the host.
Attach	Attach the selected device to the host.
Rename	Change the display name of the selected device.
Turn On LED	Turn on the locator LED for the selected devices.
Turn Off LED	Turn off the locator LED for the selected devices.
Mark as Flash Disk	Mark the selected devices as flash disks.
Mark as HDD Disk	Mark the selected devices as HDD disks.
Mark as Local	Mark the selected devices as local for the host.
Mark as Remote	Mark the selected devices as remote for the host.
Erase Partitions	Erase partitions on the selected devices.
Mark as Perennially Reserved	Mark the selected device as perennially reserved.
Unmark as Perennially Reserved	Clear the perennial reservation from the selected device.

6. Use the following tabs to access additional information and modify properties for the selected device.

Tab	Description
Properties	View device properties and characteristics. View and modify multipathing policies for the device.
Paths	Display paths available for the device. Disable or enable a selected path.
Partition Details	Displays information about partitions and their formats.

Display Storage Devices for an Adapter

Display a list of storage devices accessible through a specific storage adapter on an ESXi host.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**.

   All storage adapters installed on the host are listed in the Storage Adapters table.
4. Select the adapter from the list and click the **Devices** tab.

   Storage devices that the host can access through the adapter are displayed.

5. Use the icons to perform basic storage management tasks.

   Availability of specific icons depends on the device type and configuration.

Icon	Description
Refresh	Refresh information about storage adapters, topology, and file systems.
Detach	Detach the selected device from the host.
Attach	Attach the selected device to the host.
Rename	Change the display name of the selected device.

Comparing Types of Storage

Whether certain vSphere functionality is supported might depend on the storage technology that you use.

The following table compares networked storage technologies that ESXi supports.

Table 202: Networked Storage that ESXi Supports

Technology	Protocols	Transfers	Interface
Fibre Channel	FC/SCSI	Block access of data/LUN	FC HBA
Fibre Channel over Ethernet	FCoE/SCSI	Block access of data/LUN	• Converged Network Adapter (hardware FCoE) • NIC with FCoE support (software FCoE) **Note:** Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.
iSCSI	IP/SCSI	Block access of data/LUN	• iSCSI HBA or iSCSI-enabled NIC (hardware iSCSI) • Network adapter (software iSCSI)
NAS	IP/NFS	File (no direct LUN access)	Network adapter

The following table compares the vSphere features that different types of storage support.

Table 203: vSphere Features Supported by Storage

Storage Type	Boot VM	vMotion	Datastore	RDM	VM Cluster	vSphere HA and DRS	Storage APIs - Data Protection
Local Storage	Yes	No	VMFS	No	Yes	No	Yes
Fibre Channel	Yes	Yes	VMFS	Yes	Yes	Yes	Yes
iSCSI	Yes	Yes	VMFS	Yes	Yes	Yes	Yes
NAS over NFS	Yes	Yes	NFS 3 and NFS 4.1	No	No	Yes	Yes

Note: Local storage supports a cluster of virtual machines on a single host (also known as a cluster in a box). A shared virtual disk is required. For more information about this configuration, see the *vSphere Resource Management* documentation.

Supported Storage Adapters

Storage adapters provide connectivity for your ESXi host to a specific storage unit or network.

ESXi supports different classes of adapters, including SCSI, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE), and Ethernet. ESXi accesses the adapters directly through device drivers in the VMkernel.

Depending on the type of storage you use, you might need to enable and configure a storage adapter on your host.

For information on setting up software FCoE adapters, see Configuring Fibre Channel over Ethernet.

For information on configuring different types of iSCSI adapters, see Configuring iSCSI and iSER Adapters and Storage.

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

View Storage Adapter Information

An ESXi host uses storage adapters to access different storage devices. You can display details for the available storage adapters and review their information.

You must enable certain adapters, for example software iSCSI or FCoE, before you can view their information. To configure adapters, see the following:

- Configuring iSCSI and iSER Adapters and Storage
- Configuring Fibre Channel over Ethernet

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**.
4. Use the icons to perform storage adapter tasks.

   Availability of specific icons depends on the storage configuration.

Icon	Description
Add Software Adapter	Add a storage adapter. Applies to software iSCSI and software FCoE.
Refresh	Refresh information about storage adapters, topology, and file systems on the host.
Rescan Storage	Rescan all storage adapters on the host to discover newly added storage devices or VMFS datastores.
Rescan Adapter	Rescan the selected adapter to discover newly added storage devices.

5. To view details for a specific adapter, select the adapter from the list.
6. Use tabs under Adapter Details to access additional information and modify properties for the selected adapter.

Tab	Description
Properties	Review general adapter properties that typically include a name and model of the adapter and unique identifiers formed according to specific storage standards. For iSCSI and FCoE adapters, use this tab to configure additional properties, for example, authentication.
Devices	View storage devices the adapter can access. Use the tab to perform basic device management tasks. See Display Storage Devices for an Adapter.

Tab	Description
Paths	List and manage all paths the adapter uses to access storage devices.
Targets (Fibre Channel and iSCSI)	Review and manage targets accessed through the adapter.
Network Port Binding (iSCSI only)	Configure port binding for software and dependent hardware iSCSI adapters.
Advanced Options (iSCSI only)	Configure advanced parameters for iSCSI.

Datastore Characteristics

Datastores are logical containers, analogous to file systems, that hide specifics of each storage device and provide a uniform model for storing virtual machine files. You can display all datastores available to your hosts and analyze their properties.

Datastores are added to vCenter Server in the following ways:

- You can create a VMFS datastore, an NFS version 3 or 4.1 datastore, or a Virtual Volumes datastore using the New Datastore wizard. A vSAN datastore is automatically created when you enable vSAN.
- When you add an ESXi host to vCenter Server, all datastores on the host are added to vCenter Server.

The following table describes datastore details that you can see when you review datastores through the vSphere Client. Certain characteristic might not be available or applicable to all types of datastores.

Table 204: Datastore Information

Datastore Information	Applicable Datastore Type	Description
Name	VMFS NFS vSAN vVol	Editable name that you assign to a datastore. For information on renaming a datastore, see Change Datastore Name.
Type	VMFS NFS vSAN vVol	File system that the datastore uses. For information about VMFS and NFS datastores and how to manage them, see Working with Datastores. For information about vSAN datastores, see the *Administering VMware vSAN* documentation. For information about Virtual Volumes, see Working with VMware vSphere Virtual Volumes.
Device Backing	VMFS NFS vSAN	Information about underlying storage, such as a storage device on which the datastore is deployed (VMFS), server and folder (NFS), or disk groups (vSAN).
Protocol Endpoints	vVol	Information about corresponding protocol endpoints. See Protocol Endpoints.
Extents	VMFS	Individual extents that the datastore spans and their capacity.
Drive Type	VMFS	Type of the underlying storage device, such as a flash drive or a regular HHD drive. For details, see Working with Flash Devices.
Capacity	VMFS NFS vSAN vVol	Includes total capacity, provisioned space, and free space.

Datastore Information	Applicable Datastore Type	Description
Mount Point	VMFS NFS vSAN vVol	A path to the datastore in the `/vmfs/volumes/` directory of the host.
Capability Sets	VMFS **Note:** A multi-extent VMFS datastore assumes capabilities of only one of its extents. NFS vSAN vVol	Information about storage data services that the underlying storage entity provides. You cannot modify them.
Storage I/O Control	VMFS NFS	Information on whether cluster-wide storage I/O prioritization is enabled. See the *vSphere Resource Management* documentation.
Hardware Acceleration	VMFS NFS vSAN vVol	Information on whether the underlying storage entity supports hardware acceleration. The status can be Supported, Not Supported, or Unknown. For details, see Storage Hardware Acceleration. **Note:** NFS 4.1 does not support Hardware Acceleration.
Tags	VMFS NFS vSAN vVol	Datastore capabilities that you define and associate with datastores in a form of tags. For information, see Assign Tags to Datastores.
Connectivity with Hosts	VMFS NFS vVol	Hosts where the datastore is mounted.
Multipathing	VMFS vVol	Path selection policy the host uses to access storage. For more information, see Understanding Multipathing and Failover.

Display Datastore Information

Access the Datastores view with the vSphere Client navigator.

Use the Datastores view to list all datastores available in the vSphere infrastructure inventory, analyze the information, and modify properties.

1. Navigate to any inventory object that is a valid parent object of a datastore, such as a host, a cluster, or a data center, and click the **Datastores** tab.

   Datastores that are available in the inventory appear in the center panel.

2. Use the options from a datastore right-click menu to perform basic tasks for a selected datastore.

   Availability of specific options depends on the type of the datastore and its configuration.

Option	Description
Register VM	Register an existing virtual machine in the inventory. See the *vSphere Virtual Machine Administration* documentation.
Increase Datastore Capacity	Increase the capacity of the VMFS datastore or add an extent. See Increase VMFS Datastore Capacity.

Option	Description
Browse Files	Navigate to the datastore file browser. See Use Datastore Browser.
Rename	Change the datastore name. See Change Datastore Name.
Mount Datastore	Mount the datastore to certain hosts. See Mount Datastores.
Unmount Datastore	Unmount the datastore from certain hosts. See Unmount Datastores.
Maintenance Mode	Use datastore maintenance mode. See the *vSphere Resource Management* documentation.
Configure Storage I/O Control (VMFS)	Enable Storage I/O Control for the VMFS datastore. See the *vSphere Resource Management* documentation.
Edit Space Reclamation (VMFS)	Change space reclamation settings for the VMFS datastore. See Change Space Reclamation Settings.
Delete Datastore (VMFS)	Remove the VMFS datastore. See Remove VMFS Datastores.
Tags & Custom Attributes	Use tags to encode information about the datastore. See Assign Tags to Datastores.

3. To view specific datastore details, click a selected datastore.
4. Use tabs to access additional information and modify datastore properties.

Tab	Description
Summary	View statistics and configuration for the selected datastore.
Monitor	View alarms, performance data, resource allocation, events, and other status information for the datastore.
Configure	View and modify datastore properties. Menu items that you can see depend on the datastore type.
Permissions	Assign or edit permissions for the selected datastore.
Files	Navigate to the datastore file browser.
Hosts	View hosts where the datastore is mounted.
VMs	View virtual machines that reside on the datastore.

Using Persistent Memory Devices with ESXi

ESXi supports next generation persistent memory devices, also known as Non-Volatile Memory (NVM) devices. These devices combine performance and speed of memory with the persistence of traditional storage. They can retain stored data through reboots or power source failures.

Virtual machines that require high bandwidth, low latency, and persistence can benefit from this technology. Examples include VMs with acceleration databases and analytics workload.

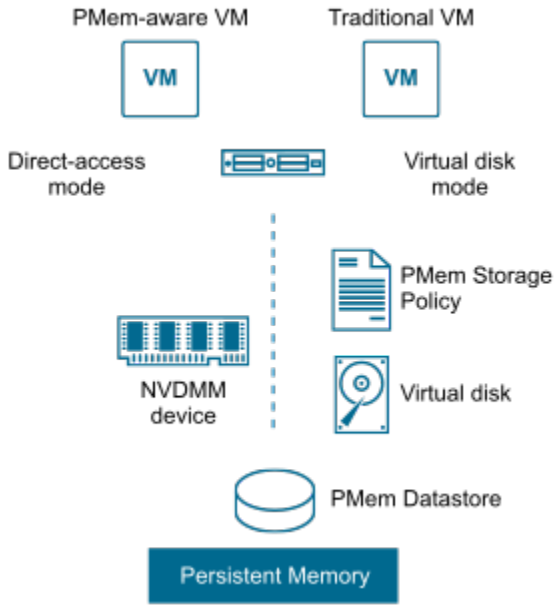
To use persistent memory with your ESXi host, you must be familiar with the following concepts.

PMem Datastore

After you add persistent memory to your ESXi host, the host detects the hardware, and then formats and mounts it as a local PMem datastore. ESXi uses VMFS-L as a file system format. Only one local PMem datastore per host is supported.

	Note: When you manage physical persistent memory, make sure to evacuate all VMs from the host and place the host into maintenance mode.
	To reduce administrative overhead, the PMem datastore offers a simplified management model. Traditional datastore tasks do not generally apply to the datastore because the host automatically performs all the required operations on the background. As an administrator, you cannot display the datastore in the Datastores view of the vSphere Client, or perform other regular datastore actions. The only operation available to you is monitoring statistics for the PMem datastore. The PMem datastore is used to store virtual NVDIMM devices and traditional virtual disks of a VM. The VM home directory with the `vmx` and `vmware.log` files cannot be placed on the PMem datastore.
PMem Access Modes	ESXi exposes persistent memory to a VM in two different modes. PMem-aware VMs can have direct access to persistent memory. Traditional VMs can use fast virtual disks stored on the PMem datastore.
Direct-Access Mode	In this mode, also called virtual PMem (vPMem) mode, a PMem region can be presented to a VM as a virtual non-volatile dual in-line memory module (NVDIMM) module. The VM uses the NVDIMM module as a standard byte-addressable memory that can persist across power cycles. You can add one or several NVDIMM modules when provisioning the VM. The VMs must be of the hardware version ESXi 6.7 or later and have a PMem-aware guest OS. The NVDIMM device is compatible with latest guest OSes that support persistent memory, for example, Windows 2016. Each NVDIMM device is automatically stored on the PMem datastore.
Virtual Disk Mode	This mode, also called virtual PMem disks (vPMemDisk) mode, is available to any traditional VM and supports any hardware version, including all legacy versions. VMs are not required to be PMem-aware. When you use this mode, you create a regular SCSI virtual disk and attach a PMem VM storage policy to the disk. The policy automatically places the disk on the PMem datastore.
PMem Storage Policy	To place the virtual disk on the PMem datastore, you must apply the host-local PMem default storage policy to the disk. The policy is not editable. The policy can be applied only to virtual disks. Because the VM home directory does not reside on the PMem datastore, make sure to place it on any standard datastore. After you assign the PMem storage policy to the virtual disk, you cannot change the policy through the **VM Edit Setting** dialog box. To change the policy, migrate or clone the VM.

The following graphic illustrates how the persistent memory components interact.



For information about how to configure and manage VMs with NVDIMMs or virtual persistent memory disks, see the *vSphere Resource Management* documentation and *vSphere Virtual Machine Administration*.

Monitor PMem Datastore Statistics

You can use the vSphere Client and the `esxcli` command to review the capacity of the PMem datastore and some of its other attributes.

However, unlike regular datastores, such as VMFS or vVol, the PMem datastore does not appear in the Datastores view of the vSphere Client. Regular datastore administrative tasks do not apply to it.

Review PMem datastore information.

Option	Description
vSphere Client	1. Navigate to the ESXi host and click **Summary**. 2. In the Hardware panel, verify that Persistent Memory is displayed and review its capacity.
esxcli command	Use the `esxcli storage filesystem list` to list the PMem datastore.

Viewing the PMem Datastore

The following sample output appears when you use the `esxcli storage filesystem list` command to list the datastore.

```
# esxcli storage filesystem list
Mount Point             Volume Name         UUID         Mounted   Type      Size           Free
----------------------  ----------------  -------------  --------  -------  ------------
 ------------

/vmfs/volumes/5xxx...     ds01-102         5xxx...       true     VMFS-6  14227079168   12718178304
/vmfs/volumes/59ex...     ds02-102         59ex...       true     VMFS-6  21206401024   19697500160
/vmfs/volumes/59bx...                      59bx...       true     vfat    4293591040    4274847744
/vmfs/volumes/pmem:5ax... PMemDS-56ax...   pmem:5a0x...  true     PMEM    12880707584   11504975872
```

Overview of Using ESXi with a SAN

Using ESXi with a SAN improves flexibility, efficiency, and reliability. Using ESXi with a SAN also supports centralized management, failover, and load balancing technologies.

The following are benefits of using ESXi with a SAN:

- You can store data securely and configure multiple paths to your storage, eliminating a single point of failure.
- Using a SAN with ESXi systems extends failure resistance to the server. When you use SAN storage, all applications can instantly be restarted on another host after the failure of the original host.
- You can perform live migration of virtual machines using VMware vMotion.
- Use VMware High Availability (HA) in conjunction with a SAN to restart virtual machines in their last known state on a different server if their host fails.
- Use VMware Fault Tolerance (FT) to replicate protected virtual machines on two different hosts. Virtual machines continue to function without interruption on the secondary host if the primary one fails.
- Use VMware Distributed Resource Scheduler (DRS) to migrate virtual machines from one host to another for load balancing. Because storage is on a shared SAN array, applications continue running seamlessly.
- If you use VMware DRS clusters, put an ESXi host into maintenance mode to have the system migrate all running virtual machines to other ESXi hosts. You can then perform upgrades or other maintenance operations on the original host.

The portability and encapsulation of VMware virtual machines complements the shared nature of this storage. When virtual machines are located on SAN-based storage, you can quickly shut down a virtual machine on one server and power it up on another server, or suspend it on one server and resume operation on another server on the same network. This ability allows you to migrate computing resources while maintaining consistent shared access.

ESXi and SAN Use Cases

When used with a SAN, ESXi can benefit from multiple vSphere features, including Storage vMotion, Distributed Resource Scheduler (DRS), High Availability, and so on.

Using ESXi with a SAN is effective for the following tasks:

Storage consolidation and simplification of storage layout	If you are working with multiple hosts, and each host is running multiple virtual machines, the storage on the hosts is no longer sufficient. You might need to use external storage. The SAN can provide a simple system architecture and other benefits.
Maintenance with zero downtime	When performing ESXi host or infrastructure maintenance, use vMotion to migrate virtual machines to other host. If shared storage is on the SAN, you can perform maintenance without interruptions to the users of the virtual machines. Virtual machine working processes continue throughout a migration.
Load balancing	You can add a host to a DRS cluster, and the host's resources become part of the cluster's resources. The distribution and use of CPU and memory resources for all hosts and virtual machines in the cluster are continuously monitored. DRS compares these metrics to an ideal resource use. The ideal use considers the attributes of the cluster's resource pools and virtual machines, the current demand, and the imbalance target. If needed, DRS performs or recommends virtual machine migrations.
Disaster recovery	You can use VMware High Availability to configure multiple ESXi hosts as a cluster. The cluster provides rapid recovery from outages and cost-effective high availability for applications running in virtual machines.
Simplified array migrations and storage upgrades	When you purchase new storage systems, use Storage vMotion to perform live migrations of virtual machines from existing storage

to their new destinations. You can perform the migrations without interruptions of the virtual machines.

Specifics of Using SAN Storage with ESXi

Using a SAN with an ESXi host differs from a traditional SAN use in several ways.

When you use SAN storage with ESXi, the following considerations apply:

- You cannot use SAN administration tools to access operating systems of virtual machines that reside on the storage. With traditional tools, you can monitor only the VMware ESXi operating system. You use the vSphere Client to monitor virtual machines.
- The HBA visible to the SAN administration tools is part of the ESXi system, not part of the virtual machine.
- Typically, your ESXi system performs multipathing for you.

ESXi Hosts and Multiple Storage Arrays

An ESXi host can access storage devices presented from multiple storage arrays, including arrays from different vendors.

When you use multiple arrays from different vendors, the following considerations apply:

- If your host uses the same SATP for multiple arrays, be careful when you change the default PSP for that SATP. The change applies to all arrays. For information on SATPs and PSPs, see Understanding Multipathing and Failover.
- Some storage arrays make recommendations on queue depth and other settings. Typically, these settings are configured globally at the ESXi host level. Changing settings for one array impacts other arrays that present LUNs to the host. For information on changing queue depth, see the VMware knowledge base article at http://kb.vmware.com/kb/1267.
- Use single-initiator-single-target zoning when zoning ESXi hosts to Fibre Channel arrays. With this type of configuration, fabric-related events that occur on one array do not impact other arrays. For more information about zoning, see Using Zoning with Fibre Channel SANs.

Making LUN Decisions

You must plan how to set up storage for your ESXi systems before you format LUNs with VMFS datastores.

When you make your LUN decision, the following considerations apply:

- Each LUN must have the correct RAID level and storage characteristic for the applications running in virtual machines that use the LUN.
- Each LUN must contain only one VMFS datastore.
- If multiple virtual machines access the same VMFS, use disk shares to prioritize virtual machines.

You might want fewer, larger LUNs for the following reasons:

- More flexibility to create virtual machines without asking the storage administrator for more space.
- More flexibility for resizing virtual disks, doing snapshots, and so on.
- Fewer VMFS datastores to manage.

You might want more, smaller LUNs for the following reasons:

- Less wasted storage space.
- Different applications might need different RAID characteristics.
- More flexibility, as the multipathing policy and disk shares are set per LUN.
- Use of Microsoft Cluster Service requires that each cluster disk resource is in its own LUN.
- Better performance because there is less contention for a single volume.

When the storage characterization for a virtual machine is unavailable, it might not be easy to determine the number and size of LUNs to provision. You can experiment using either a predictive or adaptive scheme.

Use the Predictive Scheme to Make LUN Decisions

When setting up storage for ESXi systems, before creating VMFS datastores, you must decide on the size and number of LUNs to provision. You can experiment using the predictive scheme.

1. Provision several LUNs with different storage characteristics.
2. Create a VMFS datastore on each LUN, labeling each datastore according to its characteristics.
3. Create virtual disks to contain the data for virtual machine applications in the VMFS datastores created on LUNs with the appropriate RAID level for the applications' requirements.
4. Use disk shares to distinguish high-priority from low-priority virtual machines.

   Note: Disk shares are relevant only within a given host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.
5. Run the applications to determine whether virtual machine performance is acceptable.

Use the Adaptive Scheme to Make LUN Decisions

When setting up storage for ESXi hosts, before creating VMFS datastores, you must decide on the number and size of LUNS to provision. You can experiment using the adaptive scheme.

1. Provision a large LUN (RAID 1+0 or RAID 5), with write caching enabled.
2. Create a VMFS on that LUN.
3. Create four or five virtual disks on the VMFS.
4. Run the applications to determine whether disk performance is acceptable.

If performance is acceptable, you can place additional virtual disks on the VMFS. If performance is not acceptable, create a new, large LUN, possibly with a different RAID level, and repeat the process. Use migration so that you do not lose virtual machines data when you recreate the LUN.

Selecting Virtual Machine Locations

When you are working on optimizing performance for your virtual machines, storage location is an important factor. Depending on your storage needs, you might select storage with high performance and high availability, or storage with lower performance.

Storage can be divided into different tiers depending on several factors:

- High Tier. Offers high performance and high availability. Might offer built-in snapshots to facilitate backups and point-in-time (PiT) restorations. Supports replication, full storage processor redundancy, and SAS drives. Uses high-cost spindles.
- Mid Tier. Offers mid-range performance, lower availability, some storage processor redundancy, and SCSI or SAS drives. Might offer snapshots. Uses medium-cost spindles.
- Lower Tier. Offers low performance, little internal storage redundancy. Uses low-end SCSI drives or SATA.

Not all VMs must be on the highest-performance and most-available storage throughout their entire life cycle.

When you decide where to place a virtual machine, the following considerations apply:

- Criticality of the VM
- Performance and availability requirements
- PiT restoration requirements

- Backup and replication requirements

A virtual machine might change tiers throughout its life cycle because of changes in criticality or changes in technology. Criticality is relative and might change for various reasons, including changes in the organization, operational processes, regulatory requirements, disaster planning, and so on.

Third-Party Management Applications

You can use third-party management applications with your ESXi host.

Most SAN hardware is packaged with storage management software. In many cases, this software is a Web application that can be used with any Web browser connected to your network. In other cases, this software typically runs on the storage system or on a single server, independent of the servers that use the SAN for storage.

Use this third-party management software for the following tasks:

- Storage array management, including LUN creation, array cache management, LUN mapping, and LUN security.
- Setting up replication, check points, snapshots, or mirroring.

If you run the SAN management software on a virtual machine, you gain the benefits of a virtual machine, including failover with vMotion and VMware HA. Because of the additional level of indirection, however, the management software might not see the SAN. In this case, you can use an RDM.

Note: Whether a virtual machine can run management software successfully depends on the particular storage system.

SAN Storage Backup Considerations

Having a proper backup strategy is one of the most important aspects of SAN management. In the SAN environment, backups have two goals. The first goal is to archive online data to offline media. This process is repeated periodically for all online data on a time schedule. The second goal is to provide access to offline data for recovery from a problem. For example, database recovery often requires a retrieval of archived log files that are not currently online.

Scheduling a backup depends on several factors:

- Identification of critical applications that require more frequent backup cycles within a given period.
- Recovery point and recovery time goals. Consider how precise your recovery point must be, and how long you are willing to wait for it.
- The rate of change (RoC) associated with the data. For example, if you are using synchronous/asynchronous replication, the RoC affects the amount of bandwidth required between the primary and secondary storage devices.
- Overall impact on a SAN environment, storage performance, and other applications.
- Identification of peak traffic periods on the SAN. Backups scheduled during those peak periods can slow the applications and the backup process.
- Time to schedule all backups within the data center.
- Time it takes to back up an individual application.
- Resource availability for archiving data, such as offline media access.

Include a recovery-time objective for each application when you design your backup strategy. That is, consider the time and resources necessary to perform a backup. For example, if a scheduled backup stores so much data that recovery requires a considerable amount of time, examine the scheduled backup. Perform the backup more frequently, so that less data is backed up at a time and the recovery time decreases.

If an application requires recovery within a certain time frame, the backup process must provide a time schedule and specific data processing to meet the requirement. Fast recovery can require the use of recovery volumes that reside on online storage. This process helps to minimize or eliminate the need to access slow offline media for missing data components.

Using Third-Party Backup Packages

You can use third-party backup solutions to protect system, application, and user data in your virtual machines.

The Storage APIs - Data Protection that VMware offers can work with third-party products. When using the APIs, third-party software can perform backups without loading ESXi hosts with the processing of backup tasks.

The third-party products using the Storage APIs - Data Protection can perform the following backup tasks:

- Perform a full, differential, and incremental image backup and restore of virtual machines.
- Perform a file-level backup of virtual machines that use supported Windows and Linux operating systems.
- Ensure data consistency by using Microsoft Volume Shadow Copy Services (VSS) for virtual machines that run supported Microsoft Windows operating systems.

Because the Storage APIs - Data Protection use the snapshot capabilities of VMFS, backups do not require that you stop virtual machines. These backups are nondisruptive, can be performed at any time, and do not need extended backup windows.

For information about the Storage APIs - Data Protection and integration with backup products, see the VMware website or contact your vendor.

Using ESXi with Fibre Channel SAN

When you set up ESXi hosts to use FC SAN storage arrays, special considerations are necessary. This section provides introductory information about how to use ESXi with an FC SAN array.

Fibre Channel SAN Concepts

If you are an ESXi administrator planning to set up hosts to work with SANs, you must have a working knowledge of SAN concepts. You can find information about SANs in print and on the Internet. Because this industry changes constantly, check these resources frequently.

If you are new to SAN technology, familiarize yourself with the basic terminology.

A storage area network (SAN) is a specialized high-speed network that connects host servers to high-performance storage subsystems. The SAN components include host bus adapters (HBAs) in the host servers, switches that help route storage traffic, cables, storage processors (SPs), and storage disk arrays.

A SAN topology with at least one switch present on the network forms a SAN fabric.

To transfer traffic from host servers to shared storage, the SAN uses the Fibre Channel (FC) protocol that packages SCSI commands into Fibre Channel frames.

To restrict server access to storage arrays not allocated to that server, the SAN uses zoning. Typically, zones are created for each group of servers that access a shared group of storage devices and LUNs. Zones define which HBAs can connect to which SPs. Devices outside a zone are not visible to the devices inside the zone.

Zoning is similar to LUN masking, which is commonly used for permission management. LUN masking is a process that makes a LUN available to some hosts and unavailable to other hosts.

When transferring data between the host server and storage, the SAN uses a technique known as multipathing. Multipathing allows you to have more than one physical path from the ESXi host to a LUN on a storage system.

Generally, a single path from a host to a LUN consists of an HBA, switch ports, connecting cables, and the storage controller port. If any component of the path fails, the host selects another available path for I/O. The process of detecting a failed path and switching to another is called path failover.

Ports in Fibre Channel SAN

In the context of this document, a port is the connection from a device into the SAN. Each node in the SAN, such as a host, a storage device, or a fabric component has one or more ports that connect it to the SAN. Ports are identified in a number of ways.

WWPN (World Wide Port Name)	A globally unique identifier for a port that allows certain applications to access the port. The FC switches discover the WWPN of a device or host and assign a port address to the device.
Port_ID (or port address)	Within a SAN, each port has a unique port ID that serves as the FC address for the port. This unique ID enables routing of data through the SAN to that port. The FC switches assign the port ID when the device logs in to the fabric. The port ID is valid only while the device is logged on.

When N-Port ID Virtualization (NPIV) is used, a single FC HBA port (N-port) can register with the fabric by using several WWPNs. This method allows an N-port to claim multiple fabric addresses, each of which appears as a unique entity. When ESXi hosts use a SAN, these multiple, unique identifiers allow the assignment of WWNs to individual virtual machines as part of their configuration.

Fibre Channel Storage Array Types

ESXi supports different storage systems and arrays.

The types of storage that your host supports include active-active, active-passive, and ALUA-compliant.

Active-active storage system	Supports access to the LUNs simultaneously through all the storage ports that are available without significant performance degradation. All the paths are active, unless a path fails.
Active-passive storage system	A system in which one storage processor is actively providing access to a given LUN. The other processors act as a backup for the LUN and can be actively providing access to other LUN I/O. I/O can be successfully sent only to an active port for a given LUN. If access through the active storage port fails, one of the passive storage processors can be activated by the servers accessing it.
Asymmetrical storage system	Supports Asymmetric Logical Unit Access (ALUA). ALUA-compliant storage systems provide different levels of access per port. With ALUA, the host can determine the states of target ports and prioritize paths. The host uses some of the active paths as primary, and uses others as secondary.

Using Zoning with Fibre Channel SANs

Zoning provides access control in the SAN topology. Zoning defines which HBAs can connect to which targets. When you configure a SAN by using zoning, the devices outside a zone are not visible to the devices inside the zone.

Zoning has the following effects:

- Reduces the number of targets and LUNs presented to a host.
- Controls and isolates paths in a fabric.
- Can prevent non- ESXi systems from accessing a particular storage system, and from possibly destroying VMFS data.
- Can be used to separate different environments, for example, a test from a production environment.

With ESXi hosts, use a single-initiator zoning or a single-initiator-single-target zoning. The latter is a preferred zoning practice. Using the more restrictive zoning prevents problems and misconfigurations that can occur on the SAN.

For detailed instructions and best zoning practices, contact storage array or switch vendors.

How Virtual Machines Access Data on a Fibre Channel SAN

ESXi stores a virtual machine's disk files within a VMFS datastore that resides on a SAN storage device. When virtual machine guest operating systems send SCSI commands to their virtual disks, the SCSI virtualization layer translates these commands to VMFS file operations.

When a virtual machine interacts with its virtual disk stored on a SAN, the following process takes place:

1. When the guest operating system in a virtual machine reads or writes to a SCSI disk, it sends SCSI commands to the virtual disk.
2. Device drivers in the virtual machine’s operating system communicate with the virtual SCSI controllers.
3. The virtual SCSI controller forwards the command to the VMkernel.
4. The VMkernel performs the following tasks.
   a. Locates the appropriate virtual disk file in the VMFS volume.
   b. Maps the requests for the blocks on the virtual disk to blocks on the appropriate physical device.
   c. Sends the modified I/O request from the device driver in the VMkernel to the physical HBA.
5. The physical HBA performs the following tasks.
   a. Packages the I/O request according to the rules of the FC protocol.
   b. Transmits the request to the SAN.
6. Depending on a port the HBA uses to connect to the fabric, one of the SAN switches receives the request. The switch routes the request to the appropriate storage device.

Configuring Fibre Channel Storage

When you use ESXi systems with SAN storage, specific hardware and system requirements exist.

ESXi Fibre Channel SAN Requirements

In preparation for configuring your SAN and setting up your ESXi system to use SAN storage, review the requirements and recommendations.

- Make sure that ESXi systems support the SAN storage hardware and firmware combinations you use. For an up-to-date list, see the *VMware Compatibility Guide*.
- Configure your system to have only one VMFS volume per LUN.
- Unless you are using diskless servers, do not set up the diagnostic partition on a SAN LUN.
  If you use diskless servers that boot from a SAN, a shared diagnostic partition is appropriate.
- Use RDMs to access raw disks. For information, see Raw Device Mapping.
- For multipathing to work properly, each LUN must present the same LUN ID number to all ESXi hosts.
- Make sure that the storage device driver specifies a large enough queue. You can set the queue depth for the physical HBA during a system setup.
- VMtools increases the default disk timeout SCSI `TimeoutValue` parameter to 180 seconds. On virtual machines without VMtools, increase the value of the SCSI `TimeoutValue` parameter. With this parameter set up, the VMs can better tolerate delayed I/O resulting from a path failover.

ESXi Fibre Channel SAN Restrictions

When you use ESXi with a SAN, certain restrictions apply.

- ESXi does not support FC connected tape devices.
- You cannot use multipathing software inside a virtual machine to perform I/O load balancing to a single physical LUN. However, when your Microsoft Windows virtual machine uses dynamic disks, this restriction does not apply. For information about configuring dynamic disks, see Set Up Dynamic Disk Mirroring.

Setting LUN Allocations

This topic provides general information about how to allocate LUNs when your ESXi works with SAN.

When you set LUN allocations, be aware of the following points:

Storage provisioning	To ensure that the ESXi system recognizes the LUNs at startup time, provision all LUNs to the appropriate HBAs before you connect the SAN to the ESXi system. Provision all LUNs to all ESXi HBAs at the same time. HBA failover works only if all HBAs see the same LUNs. For LUNs that are shared among multiple hosts, make sure that LUN IDs are consistent across all hosts.
vMotion and VMware DRS	When you use vCenter Server and vMotion or DRS, make sure that the LUNs for the virtual machines are provisioned to all ESXi hosts. This action provides the most ability to move virtual machines.
Active-active compared to active-passive arrays	When you use vMotion or DRS with an active-passive SAN storage device, make sure that all ESXi systems have consistent paths to all storage processors. Not doing so can cause path thrashing when a vMotion migration occurs. For active-passive storage arrays not listed in Storage/SAN Compatibility, VMware does not support storage port failover. In those cases, you must connect the server to the active port on the storage array. This configuration ensures that the LUNs are presented to the ESXi host.

Setting Fibre Channel HBAs

Typically, FC HBAs that you use on your ESXi host work correctly with the default configuration settings.

You should follow the configuration guidelines provided by your storage array vendor. During FC HBA setup, consider the following issues.

- Do not mix FC HBAs from different vendors in a single host. Having different models of the same HBA is supported, but a single LUN cannot be accessed through two different HBA types, only through the same type.
- Ensure that the firmware level on each HBA is the same.
- Set the timeout value for detecting a failover. To ensure optimal performance, do not change the default value.
- ESXi supports 32 Gbps end-to-end Fibre Channel connectivity.

Installation and Setup Steps

This topic provides an overview of installation and setup steps that you need to follow when configuring your SAN environment to work with ESXi.

Follow these steps to configure your ESXi SAN environment.

1. Design your SAN if it is not already configured. Most existing SANs require only minor modification to work with ESXi.
2. Check that all SAN components meet requirements.
3. Perform any necessary storage array modification.
   Most vendors have vendor-specific documentation for setting up a SAN to work with VMware ESXi.
4. Set up the HBAs for the hosts you have connected to the SAN.
5. Install ESXi on the hosts.
6. Create virtual machines and install guest operating systems.

7. (Optional) Set up your system for VMware HA failover or for using Microsoft Clustering Services.
8. Upgrade or modify your environment as needed.

N-Port ID Virtualization

N-Port ID Virtualization (NPIV) is an ANSI T11 standard that describes how a single Fibre Channel HBA port can register with the fabric using several worldwide port names (WWPNs). This allows a fabric-attached N-port to claim multiple fabric addresses. Each address appears as a unique entity on the Fibre Channel fabric.

How NPIV-Based LUN Access Works

NPIV enables a single FC HBA port to register several unique World Wide Name (WWN) identifiers with the fabric, each of which can be assigned to an individual virtual machine. When using NPIV, a SAN administrator can monitor and route storage access per a virtual machine.

Only virtual machines with RDMs can have WWN assignments, and they use these assignments for all RDM traffic.

When a virtual machine has a WWN assigned to it, the virtual machine's configuration file (.vmx) is updated to include a WWN pair. The WWN pair consists of a World Wide Port Name (WWPN) and a World Wide Node Name (WWNN). When that virtual machine is powered on, the VMkernel creates a virtual port (VPORT) on the physical HBA which is used to access the LUN. The VPORT is a virtual HBA that appears to the FC fabric as a physical HBA. As its unique identifier, the VPORT uses the WWN pair that was assigned to the virtual machine.

Each VPORT is specific to the virtual machine. The VPORT is destroyed on the host and no longer appears to the FC fabric when the virtual machine is powered off. When a virtual machine is migrated from one host to another, the VPORT closes on the first host and opens on the destination host.

When virtual machines do not have WWN assignments, they access storage LUNs with the WWNs of their host's physical HBAs.

Requirements for Using NPIV

If you plan to enable NPIV on your virtual machines, you should be aware of certain requirements.

- NPIV can be used only for virtual machines with RDM disks. Virtual machines with regular virtual disks use the WWNs of the host's physical HBAs.
- HBAs on your host must support NPIV.
  For information, see the *VMware Compatibility Guide* and refer to your vendor documentation.
  - Use HBAs of the same type. VMware does not support heterogeneous HBAs on the same host accessing the same LUNs.
  - If a host uses multiple physical HBAs as paths to the storage, zone all physical paths to the virtual machine. This is required to support multipathing even though only one path at a time will be active.
  - Make sure that physical HBAs on the host can detect all LUNs that are to be accessed by NPIV-enabled virtual machines running on that host.
- The switches in the fabric must be NPIV-aware.
- When configuring a LUN for NPIV access at the storage level, make sure that the NPIV LUN number and NPIV target ID match the physical LUN and Target ID.
- Zone the NPIV WWPNs so that they connect to all storage systems the cluster hosts can access, even if the VM does not use the storage. If you add any new storage systems to a cluster with one or more NPIV-enabled VMs, add the new zones, so the NPIV WWPNs can detect the new storage system target ports.

NPIV Capabilities and Limitations

Learn about specific capabilities and limitations of the use of NPIV with ESXi.

ESXi with NPIV supports the following items:

- NPIV supports vMotion. When you use vMotion to migrate a virtual machine it retains the assigned WWN.
  If you migrate an NPIV-enabled virtual machine to a host that does not support NPIV, VMkernel reverts to using a physical HBA to route the I/O.
- If your FC SAN environment supports concurrent I/O on the disks from an active-active array, the concurrent I/O to two different NPIV ports is also supported.

When you use ESXi with NPIV, the following limitations apply:

- Because the NPIV technology is an extension to the FC protocol, it requires an FC switch and does not work on the direct attached FC disks.
- When you clone a virtual machine or template with a WWN assigned to it, the clones do not retain the WWN.
- NPIV does not support Storage vMotion.
- Disabling and then re-enabling the NPIV capability on an FC switch while virtual machines are running can cause an FC link to fail and I/O to stop.

Configure or Modify WWN Assignments

Assign WWN settings to virtual machine. You can later modify the WWN assignments.

- Before configuring WWN, ensure that the ESXi host can access the storage LUN access control list (ACL) configured on the array side.
- If you want to edit the existing WWNs, power off the virtual machine.

You can create from 1 to 16 WWN pairs, which can be mapped to the first 1 to 16 physical FC HBAs on the host.

Typically, you do not need to change existing WWN assignments on your virtual machine. In certain circumstances, for example, when manually assigned WWNs are causing conflicts on the SAN, you might need to change or remove WWNs.

1. Right-click the virtual machine in the inventory and select **Edit Settings**.
2. Click **VM Options** and expand **Fibre Channel NPIV**.
3. Create or edit the WWN assignments by selecting one of the following options:

Option	Description
Temporarily disable NPIV for this virtual machine	Disable but do not remove the existing WWN assignments for the virtual machine.
Leave unchanged	Retain the existing WWN assignments. The read-only WWN assignments section displays the node and port values of any existing WWN assignments.
Generate new WWNs	Generate new WWNs, overwriting any existing WWNs. The WWNs of the HBA are not affected. Specify the number of WWNNs and WWPNs. A minimum of two WWPNs are required to support failover with NPIV. Typically only one WWNN is created for each virtual machine.
Remove WWN assignment	Remove the WWNs assigned to the virtual machine. The virtual machine uses the HBA WWNs to access the storage LUN.

4. Click **OK** to save your changes.

Register newly created WWNs in the fabric.

Configuring Fibre Channel over Ethernet

To access Fibre Channel storage, an ESXi host can use the Fibre Channel over Ethernet (FCoE) protocol.

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

The FCoE protocol encapsulates Fibre Channel frames into Ethernet frames. As a result, your host does not need special Fibre Channel links to connect to Fibre Channel storage. The host can use 10 Gbit lossless Ethernet to deliver Fibre Channel traffic.

Fibre Channel over Ethernet Adapters

To use Fibre Channel over Ethernet (FCoE), configure appropriate adapters on your host.

The adapters that VMware supports generally fall into two categories, hardware FCoE adapters and software FCoE adapters that use the native FCoE stack in ESXi.

For information on adapters that can be used with VMware FCoE, see the *VMware Compatibility Guide*

Hardware FCoE Adapters

This category includes a specialized offloaded Converged Network Adapters (CNAs) that contain network and Fibre Channel functionalities on the same card.

When such adapter is installed, your host detects and can use both CNA components. In the vSphere Client, the networking component appears as a standard network adapter (vmnic) and the Fibre Channel component as a FCoE adapter (vmhba). You do not need to configure the hardware FCoE adapter to use it.

Software FCoE Adapters

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

A software FCoE adapter uses the native FCoE protocol stack in ESXi to perform some of the FCoE processing. You must use the software FCoE adapter with a compatible NIC.

VMware supports two categories of NICs with the software FCoE adapters.

NICs With Partial FCoE Offload	The extent of the offload capabilities might depend on the type of the NIC. Generally, the NICs offer Data Center Bridging (DCB) and I/O offload capabilities.
NICs Without FCoE Offload	Any NICs that offer Data Center Bridging (DCB) and have a minimum speed of 10 Gbps. The network adapters are not required to support any FCoE offload capabilities.

Unlike the hardware FCoE adapter, the software adapter must be activated. Before you activate the adapter, you must properly configure networking.

Note: The number of software FCoE adapters you activate corresponds to the number of physical NIC ports. ESXi supports a maximum of four software FCoE adapters on one host.

Configuration Guidelines for Software FCoE

When setting up your network environment to work with ESXi software FCoE, follow the guidelines and best practices that VMware offers.

Network Switch Guidelines

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

Follow these guidelines when you configure a network switch for software FCoE environment:

- On the ports that communicate with your ESXi host, disable the Spanning Tree Protocol (STP). Having the STP enabled might delay the FCoE Initialization Protocol (FIP) response at the switch and cause an all paths down (APD) condition.
  The FIP is a protocol that FCoE uses to discover and initialize FCoE entities on the Ethernet.
- Turn on Priority-based Flow Control (PFC) and set it to AUTO.
- Make sure that you have a compatible firmware version on the FCoE switch.
- Set the MTU on the vSwitch to 2500 or more.

Network Adapter Guidelines and Best Practices

If you plan to enable software FCoE adapters to work with network adapters, specific considerations apply.

- Whether you use a partially offloaded NIC or a non-FCoE capable NIC, make sure that the latest microcode is installed on the network adapter.
- If you use the non-FCoE capable NIC, make sure that it has the DCB capability for software FCoE enablement.
- If the network adapter has multiple ports, when configuring networking, add each port to a separate vSwitch. This practice helps you to avoid an APD condition when a disruptive event, such as an MTU change, occurs.
- Do not move a network adapter port from one vSwitch to another when FCoE traffic is active. If you make this change, reboot your host afterwards.
- If you changed the vSwitch for a network adapter port and caused a failure, moving the port back to the original vSwitch resolves the problem.

Set Up Networking for Software FCoE

Before you activate the software FCoE adapters on your ESXi host, create VMkernel network adapters for all physical FCoE NICs installed on the host.

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

This procedure explains how to create a single VMkernel network adapter connected to a single FCoE physical network adapter through a vSphere Standard switch. If your host has multiple network adapters or multiple ports on the adapter, connect each FCoE NIC to a separate standard switch. For more information, see the *vSphere Networking* documentation.

1. In the vSphere Client, navigate to the ESXi host.
2. Click **Actions** > **Add Networking**.
3. Select **VMkernel Network Adapter**, and click **Next**.
4. Select **New standard switch** to create a vSphere Standard switch.
5. To enable Jumbo Frames, change **MTU (Bytes)** to the value of 2500 or more, and click **Next**.
6. Click the **Add adapters** icon, and select the network adapter (vmnic#) that supports FCoE.
   Make sure to assign the adapter to Active Adapters.
7. Enter a network label.
   Network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, FCoE.
8. Specify a VLAN ID and click **Next**.
   FCoE traffic requires an isolated network. Make sure that the VLAN ID you enter is different from the one used for regular networking on your host. For more information, see the *vSphere Networking* documentation.
9. After you finish configuration, review the information and click **Finish**.

You have created the virtual VMkernel adapter for the physical FCoE network adapter installed on your host.

Note: To avoid FCoE traffic disruptions, do not remove the FCoE network adapter (vmnic#) from the vSphere Standard switch after you set up FCoE networking.

Add Software FCoE Adapters

You must activate software FCoE adapters so that your ESXi host can use them to access Fibre Channel storage.

Set up networking for the software FCoE adapter.

Note: Starting from vSphere 7.0, VMware no longer supports software FCoE in production environments.

The number of software FCoE adapters you can activate corresponds to the number of physical FCoE NIC ports on your host. ESXi supports the maximum of four software FCoE adapters on one host.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and click the **Add Software Adapter** icon.
4. Select **Software FCoE Adapter**.
5. On the Add Software FCoE Adapter dialog box, select an appropriate vmnic from the drop-down list of physical network adapters.

   Only those adapters that are not yet used for FCoE traffic are listed.
6. Click **OK**.

   The software FCoE adapter appears on the list of storage adapters.

After you activate the software FCoE adapter, you can view its properties. If you do not use the adapter, you can remove it from the list of adapters.

Booting ESXi from Fibre Channel SAN

When you set up your host to boot from a SAN, your host's boot image is stored on one or more LUNs in the SAN storage system. When the host starts, it boots from the LUN on the SAN rather than from its local disk.

ESXi supports booting through a Fibre Channel host bus adapter (HBA) or a Fibre Channel over Ethernet (FCoE) converged network adapter (CNA).

Boot from SAN Benefits

Boot from SAN can provide numerous benefits to your ESXi environment. However, in certain cases, boot from SAN is not compatible with your hosts. Before you set up your system for boot from SAN, decide whether it is appropriate for your environment.

CAUTION: When you use boot from SAN with multiple ESXi hosts, each host must have its own boot LUN. If you configure multiple hosts to share the boot LUN, ESXi image corruption might occur.

If you use boot from SAN, the benefits for your environment include the following:

- Cheaper servers. Servers can be more dense and run cooler without internal storage.
- Easier server replacement. You can replace servers and have the new server point to the old boot location.
- Less wasted space. Servers without local disks often take up less space.
- Easier backup processes. You can back up the system boot images in the SAN as part of the overall SAN backup procedures. Also, you can use advanced array features such as snapshots on the boot image.
- Improved management. Creating and managing the operating system image is easier and more efficient.
- Better reliability. You can access the boot disk through multiple paths, which protects the disk from being a single point of failure.

Requirements and Considerations when Booting from Fibre Channel SAN

Your ESXi boot configuration must meet specific requirements.

Table 205: Boot from SAN Requirements

Requirement	Description
ESXi system requirements	Follow vendor recommendations for the server booting from a SAN.
Adapter requirements	Configure the adapter, so it can access the boot LUN. See your vendor documentation.
Access control	• Each host must have access to its own boot LUN only, not the boot LUNs of other hosts. Use storage system software to make sure that the host accesses only the designated LUNs. • Multiple servers can share a diagnostic partition. You can use array-specific LUN masking to achieve this configuration.
Multipathing support	Multipathing to a boot LUN on active-passive arrays is not supported because the BIOS does not support multipathing and is unable to activate a standby path.
SAN considerations	If the array is not certified for a direct connect topology, the SAN connections must be through a switched topology. If the array is certified for the direct connect topology, the SAN connections can be made directly to the array. Boot from SAN is supported for both switched topology and direct connect topology.
Hardware- specific considerations	If you are running an IBM eServer BladeCenter and use boot from SAN, you must disable IDE drives on the blades.

Getting Ready for Boot from SAN

When you prepare your ESXi host to boot from a SAN, you perform several tasks.

This section describes the generic boot-from-SAN enablement process on the rack-mounted servers. For information on enabling the boot from SAN option on Cisco Unified Computing System FCoE blade servers, refer to Cisco documentation.

Configure SAN Components and Storage System

Before you set up your ESXi host to boot from a SAN LUN, configure SAN components and a storage system.

Because configuring the SAN components is vendor-specific, refer to the product documentation for each item.

1. Connect network cable, referring to any cabling guide that applies to your setup.
   Check the switch wiring, if there is any.
2. Configure the storage array.
   a) From the SAN storage array, make the ESXi host visible to the SAN. This process is often called creating an object.
   b) From the SAN storage array, set up the host to have the WWPNs of the host's adapters as port names or node names.
   c) Create LUNs.
   d) Assign LUNs.
   e) Record the IP addresses of the switches and storage arrays.
   f) Record the WWPN for each SP.

   CAUTION: If you use a scripted installation process to install ESXi in boot from SAN mode, take special steps to avoid unintended data loss.

Configure Storage Adapter to Boot from SAN

When you set up your host to boot from SAN, you enable the boot adapter in the host BIOS. You then configure the boot adapter to initiate a primitive connection to the target boot LUN.

Determine the WWPN for the storage adapter.

Configure the storage adapter to boot from SAN.

Because configuring boot adapters is vendor-specific, consult your vendor documentation.

Set Up Your System to Boot from Installation Media

When setting up your host to boot from SAN, you first boot the host from the VMware installation media. To boot from the installation media, change the system boot sequence in the BIOS setup.

Because changing the boot sequence in the BIOS is vendor-specific, refer to vendor documentation for instructions. The following procedure explains how to change the boot sequence on an IBM host.

1. Power on your system and enter the system BIOS Configuration/Setup Utility.
2. Select **Startup Options** and press Enter.
3. Select **Startup Sequence Options** and press Enter.
4. Change the **First Startup Device** to **[CD-ROM]**.

You can now install ESXi.

Configure Emulex HBA to Boot from SAN

Configuring the Emulex HBA BIOS to boot from SAN includes enabling the BootBIOS prompt and enabling BIOS.

Enable the BootBIOS Prompt

When you configure the Emulex HBA BIOS to boot ESXi from SAN, you need to enable the BootBIOS prompt.

1. Run `lputil`.
2. Select **3. Firmware Maintenance**.
3. Select an adapter.
4. Select **6. Boot BIOS Maintenance**.
5. Select **1. Enable Boot BIOS**.

Enable the BIOS

When you configure the Emulex HBA BIOS to boot ESXi from SAN, you must enable BIOS.

1. Reboot the host.
2. To configure the adapter parameters, press ALT+E at the Emulex prompt and follow these steps.
   a) Select an adapter (with BIOS support).
   b) Select **2. Configure This Adapter's Parameters.**
   c) Select **1. Enable or Disable BIOS.**
   d) Select **1** to enable BIOS.
   e) Select **x** to exit and **Esc** to return to the previous menu.
3. To configure the boot device, follow these steps from the Emulex main menu.
   a) Select the same adapter.
   b) Select **1. Configure Boot Devices.**
   c) Select the location for the Boot Entry.
   d) Enter the two-digit boot device.
   e) Enter the two-digit (HEX) starting LUN (for example, `08`).
   f) Select the boot LUN.
   g) Select **1. WWPN.** (Boot this device using WWPN, not DID).
   h) Select **x** to exit and **Y** to reboot.
4. Boot into the system BIOS and move Emulex first in the boot controller sequence.
5. Reboot and install on a SAN LUN.

Configure QLogic HBA to Boot from SAN

This sample procedure explains how to configure the QLogic HBA to boot ESXi from SAN. The procedure involves enabling the QLogic HBA BIOS, enabling the selectable boot, and selecting the boot LUN.

1. While booting the server, press **Ctrl+Q** to enter the Fast!UTIL configuration utility.
2. Perform the appropriate action depending on the number of HBAs.

Option	Description
One HBA	If you have only one HBA, the Fast!UTIL Options page appears. Skip to Step 3.
Multiple HBAs	If you have more than one HBA, select the HBA manually. 1. In the Select Host Adapter page, use the arrow keys to position the pointer on the appropriate HBA. 2. Press **Enter**.

3. In the Fast!UTIL Options page, select **Configuration Settings** and press **Enter**.
4. In the Configuration Settings page, select **Adapter Settings** and press **Enter**.
5. Set the BIOS to search for SCSI devices.
   a) In the Host Adapter Settings page, select **Host Adapter BIOS**.
   b) Press **Enter** to toggle the value to **Enabled**.
   c) Press **Esc** to exit.
6. Enable the selectable boot.
   a) Select **Selectable Boot Settings** and press **Enter**.
   b) In the Selectable Boot Settings page, select **Selectable Boot**.
   c) Press **Enter** to toggle the value to **Enabled**.
7. Select the Boot Port Name entry in the list of storage processors (SPs) and press **Enter**.
   The Select Fibre Channel Device page opens.
8. Select the specific SP and press **Enter**.
   If you are using an active-passive storage array, the selected SP must be on the preferred (active) path to the boot LUN. If you are not sure which SP is on the active path, use your storage array management software to find out. The target IDs are created by the BIOS and might change with each reboot.
9. Perform the appropriate action depending on the number of LUNs attached to the SP.

Option	Description
One LUN	The LUN is selected as the boot LUN. You do not need to enter the Select LUN page.
Multiple LUNs	The Select LUN page opens. Use the pointer to select the boot LUN, then press **Enter**.

10. If any remaining storage processors show in the list, press **C** to clear the data.
11. Press **Esc** twice to exit and press **Enter** to save the setting.

Booting ESXi with Software FCoE

ESXi supports booting from FCoE capable network adapters.

Only NICs with partial FCoE offload support the boot capabilities with the software FCoE. If you use the NICs without FCoE offload, the software FCoE boot is not supported.

When you install and boot ESXi from an FCoE LUN, the host can use a VMware software FCoE adapter and a network adapter with FCoE capabilities. The host does not require a dedicated FCoE HBA.

You perform most configurations through the `option ROM` of your network adapter. The network adapters must support one of the following formats, which communicate parameters about an FCoE boot device to VMkernel.

- FCoE Boot Firmware Table (FBFT). FBFT is Intel propriety.
- FCoE Boot Parameter Table (FBPT). FBPT is defined by VMware for third-party vendors to implement a software FCoE boot.

The configuration parameters are set in the `option ROM` of your adapter. During an ESXi installation or a subsequent boot, these parameters are exported in to system memory in either FBFT format or FBPT format. The VMkernel can read the configuration settings and use them to access the boot LUN.

Requirements and Considerations for Software FCoE Boot

When you boot the ESXi host from SAN using software FCoE, certain requirements and considerations apply.

Requirements

- Use ESXi of a compatible version.
- The network adapter must have the following capabilities:
  - Be FCoE capable.
  - Support ESXi open FCoE stack.
  - Contain FCoE boot firmware which can export boot information in FBFT format or FBPT format.

Considerations

- You cannot change software FCoE boot configuration from within ESXi.
- Coredump is not supported on any software FCoE LUNs, including the boot LUN.
- Multipathing is not supported at pre-boot.
- Boot LUN cannot be shared with other hosts even on shared storage. Make sure that the host has access to the entire boot LUN.

Set Up Software FCoE Boot

Your ESXi host can boot from a FCoE LUN using the software FCoE adapter and a network adapter.

The network adapter has the following capabilities:

- Support partial FCoE offloads (software FCoE).
- Contain either a FCoE Boot Firmware Table (FBFT) or a FCoE Boot Parameter Table (FBPT).

For information about network adapters that support software FCoE boot, see the *VMware Compatibility Guide*.

When you configure your host for a software FCoE boot, you perform several tasks.

Configure Software FCoE Boot Parameters

To support a software FCoE boot process, a network adapter on your host must have a specially configured FCoE boot firmware. When you configure the firmware, you enable the adapter for the software FCoE boot and specify the boot LUN parameters.

In the option ROM of the network adapter, specify software FCoE boot parameters.

These parameters include a boot target, boot LUN, VLAN ID, and so on.

Because configuring the network adapter is vendor-specific, review your vendor documentation for instructions.

Install and Boot ESXifrom Software FCoE LUN

When you set up your system to boot from a software FCoE LUN, you install the ESXiimage to the target LUN. You can then boot your host from that LUN.

- Configure the `option ROM` of the network adapter, so that it points to a target boot LUN. Make sure that you have information about the bootable LUN.

- Change the boot order in the system BIOS to the following sequence:
  a. The network adapter that you use for the software FCoE boot.
  b. The ESXi installation media.
  See the vendor documentation for your system.

1. Start an interactive installation from the ESXiinstallation media.

   The ESXi installer verifies that FCoE boot is enabled in the BIOS and, if needed, creates a standard virtual switch for the FCoE capable network adapter. The name of the vSwitch is VMware_FCoE_vSwitch. The installer then uses preconfigured FCoE boot parameters to discover and display all available FCoE LUNs.
2. On the **Select a Disk** page, select the software FCoE LUN that you specified in the boot parameter setting.

   If the boot LUN does not appear in this menu, make sure that you correctly configured boot parameters in the `option ROM` of the network adapter.
3. Complete the installation by following the prompts.
4. Reboot the host.
5. Change the boot order in the system BIOS so that the FCoE boot LUN is the first bootable device.

   ESXi continues booting from the software FCoE LUN until it is ready to be used.

If needed, you can rename and modify the VMware_FCoE_vSwitch that the installer automatically created. Make sure that the Cisco Discovery Protocol (CDP) mode is set to Listen or Both.

Troubleshooting Boot from Software FCoE for an ESXi Host

If the installation or boot of ESXi from a software FCoE LUN fails, you can use several troubleshooting methods.

When you install or boot ESXi from FCoE storage, the installation or the boot process fails. The FCoE setup that you use includes a VMware software FCoE adapter and a network adapter with partial FCoE offload capabilities.

- Make sure that you correctly configured boot parameters in the option ROM of the FCoE network adapter.
- During installation, monitor the BIOS of the FCoE network adapter for any errors.
- If possible, check the VMkernel log for errors.
- Use the `esxcli` command to verify whether the boot LUN is present.
  `esxcli`*`conn_options`*`hardware bootdevice list`

Best Practices for Fibre Channel Storage

When using ESXi with Fibre Channel SAN, follow recommendations to avoid performance problems.

The vSphere Client offers extensive facilities for collecting performance information. The information is graphically displayed and frequently updated.

You can also use the `resxtop` or `esxtop` command-line utilities. The utilities provide a detailed look at how ESXi uses resources. For more information, see the *vSphere Resource Management* documentation.

Check with your storage representative if your storage system supports Storage API - Array Integration hardware acceleration features. If it does, refer to your vendor documentation to enable hardware acceleration support on the storage system side. For more information, see Storage Hardware Acceleration.

Preventing Fibre Channel SAN Problems

When you use ESXi with a Fibre Channel SAN, follow specific guidelines to avoid SAN problems.

To prevent problems with your SAN configuration, observe these tips:

- Place only one VMFS datastore on each LUN.

- Do not change the path policy the system sets for you unless you understand the implications of making such a change.
- Document everything. Include information about zoning, access control, storage, switch, server and FC HBA configuration, software and firmware versions, and storage cable plan.
- Plan for failure:
  - Make several copies of your topology maps. For each element, consider what happens to your SAN if the element fails.
  - Verify different links, switches, HBAs, and other elements to ensure that you did not miss a critical failure point in your design.
- Ensure that the Fibre Channel HBAs are installed in the correct slots in the host, based on slot and bus speed. Balance PCI bus load among the available buses in the server.
- Become familiar with the various monitor points in your storage network, at all visibility points, including host's performance charts, FC switch statistics, and storage performance statistics.
- Be cautious when changing IDs of the LUNs that have VMFS datastores being used by your ESXi host. If you change the ID, the datastore becomes inactive and its virtual machines fail. Resignature the datastore to make it active again. See Managing Duplicate VMFS Datastores.

  After you change the ID of the LUN, rescan the storage to reset the ID on your host. For information on using the rescan, see Storage Rescan Operations.

Disable Automatic ESXi Host Registration

Certain storage arrays require that ESXi hosts register with the arrays. ESXi performs automatic host registration by sending the host's name and IP address to the array. If you prefer to perform manual registration using storage management software, disable the ESXi auto-registration feature.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. Under Advanced System Settings, select the **Disk.EnableNaviReg** parameter and click the **Edit** icon.
5. Change the value to 0.

This operation disables the automatic host registration that is enabled by default.

Optimizing Fibre Channel SAN Storage Performance

Several factors contribute to optimizing a typical SAN environment.

If the environment is properly configured, the SAN fabric components (particularly the SAN switches) are only minor contributors because of their low latencies relative to servers and storage arrays. Make sure that the paths through the switch fabric are not saturated, that is, that the switch fabric is running at the highest throughput.

Storage Array Performance

Storage array performance is one of the major factors contributing to the performance of the entire SAN environment.

If you encounter any problems with storage array performance, consult your storage array vendor documentation for any relevant information.

To improve the array performance in the vSphere environment, follow these general guidelines:

- When assigning LUNs, remember that several hosts might access the LUN, and that several virtual machines can run on each host. One LUN used by a host can service I/O from many different applications running on different operating

systems. Because of this diverse workload, the RAID group containing the ESXi LUNs typically does not include LUNs used by other servers that are not running ESXi.
- Make sure that the read/write caching is available.
- SAN storage arrays require continual redesign and tuning to ensure that I/O is load-balanced across all storage array paths. To meet this requirement, distribute the paths to the LUNs among all the SPs to provide optimal load-balancing. Close monitoring indicates when it is necessary to rebalance the LUN distribution.

  Tuning statically balanced storage arrays is a matter of monitoring the specific performance statistics, such as I/O operations per second, blocks per second, and response time. Distributing the LUN workload to spread the workload across all the SPs is also important.

  Note: Dynamic load-balancing is not currently supported with ESXi.

Server Performance with Fibre Channel

You must consider several factors to ensure optimal server performance.

Each server application must have access to its designated storage with the following conditions:

- High I/O rate (number of I/O operations per second)
- High throughput (megabytes per second)
- Minimal latency (response times)

Because each application has different requirements, you can meet these goals by selecting an appropriate RAID group on the storage array.

To achieve performance goals, follow these guidelines:

- Place each LUN on a RAID group that provides the necessary performance levels. Monitor the activities and resource use of other LUNs in the assigned RAID group. A high-performance RAID group that has too many applications doing I/O to it might not meet performance goals required by an application running on the ESXi host.
- Ensure that each host has enough HBAs to increase throughput for the applications on the host for the peak period. I/O spread across multiple HBAs provides faster throughput and less latency for each application.
- To provide redundancy for a potential HBA failure, make sure that the host is connected to a dual redundant fabric.
- When allocating LUNs or RAID groups for ESXi systems, remember that multiple operating systems use and share that resource. The LUN performance required by the ESXi host might be much higher than when you use regular physical machines. For example, if you expect to run four I/O intensive applications, allocate four times the performance capacity for the ESXi LUNs.
- When you use multiple ESXi systems in with vCenter Server, the performance requirements for the storage subsystem increase correspondingly.
- The number of outstanding I/Os needed by applications running on the ESXi system must match the number of I/Os the HBA and storage array can handle.

Using ESXi with iSCSI SAN

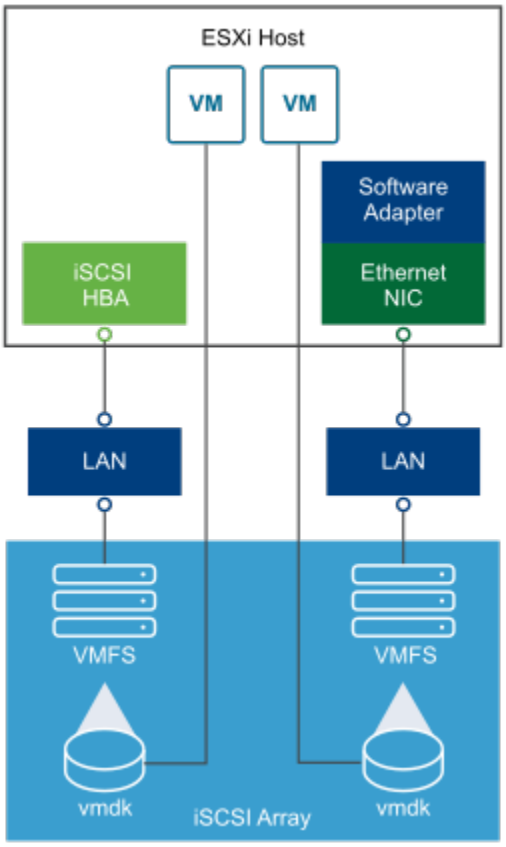
ESXi can connect to external SAN storage using the Internet SCSI (iSCSI) protocol. In addition to traditional iSCSI, ESXi also supports iSCSI Extensions for RDMA (iSER).

When the iSER protocol is enabled, the host can use the same iSCSI framework, but replaces the TCP/IP transport with the Remote Direct Memory Access (RDMA) transport.

About iSCSI SAN

iSCSI SANs use Ethernet connections between hosts and high-performance storage subsystems.

On the host side, the iSCSI SAN components include iSCSI host bus adapters (HBAs) or Network Interface Cards (NICs). The iSCSI network also includes switches and routers that transport the storage traffic, cables, storage processors (SPs), and storage disk systems.



The iSCSI SAN uses a client-server architecture.

The client, called iSCSI initiator, operates on your ESXi host. It initiates iSCSI sessions by issuing SCSI commands and transmitting them, encapsulated into the iSCSI protocol, to an iSCSI server. The server is known as an iSCSI target. Typically, the iSCSI target represents a physical storage system on the network.

The target can also be a virtual iSCSI SAN, for example, an iSCSI target emulator running in a virtual machine. The iSCSI target responds to the initiator's commands by transmitting required iSCSI data.

iSCSI Multipathing

When transferring data between the host server and storage, the SAN uses a technique known as multipathing. With multipathing, your ESXi host can have more than one physical path to a LUN on a storage system.

Generally, a single path from a host to a LUN consists of an iSCSI adapter or NIC, switch ports, connecting cables, and the storage controller port. If any component of the path fails, the host selects another available path for I/O. The process of detecting a failed path and switching to another is called path failover.

For more information on multipathing, see Understanding Multipathing and Failover.

Nodes and Ports in the iSCSI SAN

A single discoverable entity on the iSCSI SAN, such as an initiator or a target, represents an iSCSI node.

Each node has a node name. ESXi uses several methods to identify a node.

IP Address	Each iSCSI node can have an IP address associated with it so that routing and switching equipment on your network can establish the connection between the host and storage. This address is like the IP address that you assign to your computer to get access to your company's network or the Internet.
iSCSI Name	A worldwide unique name for identifying the node. iSCSI uses the iSCSI Qualified Name (IQN) and Extended Unique Identifier (EUI). By default, ESXi generates unique iSCSI names for your iSCSI initiators, for example, `iqn.1998-01.com.vmware:iscsitestox-68158ef2`. Usually, you do not have to change the default value, but if you do, make sure that the new iSCSI name you enter is worldwide unique.
iSCSI Alias	A more manageable name for an iSCSI device or port used instead of the iSCSI name. iSCSI aliases are not unique and are intended to be a friendly name to associate with a port.

Each node has one or more ports that connect it to the SAN. iSCSI ports are end-points of an iSCSI session.

iSCSI Naming Conventions

iSCSI uses a special unique name to identify an iSCSI node, either target or initiator.

iSCSI names are formatted in two different ways. The most common is the IQN format.

For more details on iSCSI naming requirements and string profiles, see RFC 3721 and RFC 3722 on the IETF website.

iSCSI Qualified Name Format

The iSCSI Qualified Name (IQN) format takes the form `iqn.yyyy-mm.naming-authority:unique` name, where:

- *`yyyy-mm`* is the year and month when the naming authority was established.
- *`naming-authority`* is the reverse syntax of the Internet domain name of the naming authority. For example, the `iscsi.vmware.com` naming authority can have the iSCSI qualified name form of `iqn.1998-01.com.vmware.iscsi`. The name indicates that the `vmware.com` domain name was registered in January of 1998, and `iscsi` is a subdomain, maintained by `vmware.com`.
- *`unique name`* is any name you want to use, for example, the name of your host. The naming authority must make sure that any names assigned following the colon are unique, such as:
  - `iqn.1998-01.com.vmware.iscsi:name1`
  - `iqn.1998-01.com.vmware.iscsi:name2`
  - `iqn.1998-01.com.vmware.iscsi:name999`

Enterprise Unique Identifier Format

The Enterprise Unique Identifier (EUI) format takes the form `eui.16_hex_digits`.

For example, `eui.0123456789ABCDEF`.

The 16-hexadecimal digits are text representations of a 64-bit number of an IEEE EUI (extended unique identifier) format. The top 24 bits are a company ID that IEEE registers with a particular company. The remaining 40 bits are assigned by the entity holding that company ID and must be unique.

iSCSI Initiators

To access iSCSI targets, your ESXi host uses iSCSI initiators.

The initiator is a software or hardware installed on your ESXi host. The iSCSI initiator originates communication between your host and an external iSCSI storage system and sends data to the storage system.

In the ESXi environment, iSCSI adapters configured on your host play the role of initiators. ESXi supports several types of iSCSI adapters.

For information on configuring and using iSCSI adapters, see Configuring iSCSI and iSER Adapters and Storage.

Software iSCSI Adapter

A software iSCSI adapter is a VMware code built into the VMkernel. Using the software iSCSI adapter, your host can connect to the iSCSI storage device through standard network adapters. The software iSCSI adapter handles iSCSI processing while communicating with the network adapter. With the software iSCSI adapter, you can use iSCSI technology without purchasing specialized hardware.

Hardware iSCSI Adapter

A hardware iSCSI adapter is a third-party adapter that offloads iSCSI and network processing from your host. Hardware iSCSI adapters are divided into categories.

Dependent Hardware iSCSI Adapter	Depends on VMware networking, and iSCSI configuration and management interfaces provided by VMware. This type of adapter can be a card that presents a standard network adapter and iSCSI offload functionality for the same port. The iSCSI offload functionality depends on the host's network configuration to obtain the IP, MAC, and other parameters used for iSCSI sessions. An example of a dependent adapter is the iSCSI licensed Broadcom 5709 NIC.
Independent Hardware iSCSI Adapter	Implements its own networking and iSCSI configuration and management interfaces. Typically, an independent hardware iSCSI adapter is a card that either presents only iSCSI offload functionality or iSCSI offload functionality and standard NIC functionality. The iSCSI offload functionality has independent configuration management that assigns the IP, MAC, and other parameters used for the iSCSI sessions. An example of an independent adapter is the QLogic QLA4052 adapter.

Hardware iSCSI adapters might need to be licensed. Otherwise, they might not appear in the client or vSphere CLI. Contact your vendor for licensing information.

Using iSER Protocol with ESXi

In addition to traditional iSCSI, ESXi supports the iSCSI Extensions for RDMA (iSER) protocol. When the iSER protocol is enabled, the iSCSI framework on the ESXi host can use the Remote Direct Memory Access (RDMA) transport instead of TCP/IP.

The traditional iSCSI protocol carries SCSI commands over a TCP/IP network between an iSCSI initiator on a host and an iSCSI target on a storage device. The iSCSI protocol encapsulates the commands and assembles that data in packets for the TCP/IP layer. When the data arrives, the iSCSI protocol disassembles the TCP/IP packets, so that the SCSI commands can be differentiated and delivered to the storage device.

iSER differs from traditional iSCSI as it replaces the TCP/IP data transfer model with the Remote Direct Memory Access (RDMA) transport. Using the direct data placement technology of the RDMA, the iSER protocol can transfer data

directly between the memory buffers of the ESXi host and storage devices. This method eliminates unnecessary TCP/IP processing and data copying, and can also reduce latency and the CPU load on the storage device.

In the iSER environment, iSCSI works exactly as before, but uses an underlying RDMA fabric interface instead of the TCP/IP-based interface.

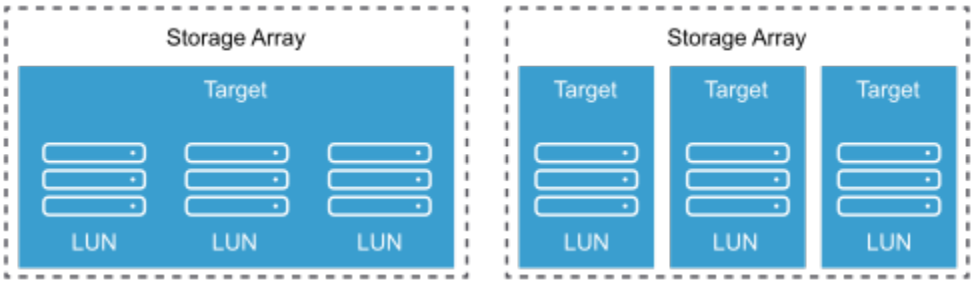
Because the iSER protocol preserves the compatibility with iSCSI infrastructure, the process of enabling iSER on the ESXi host is similar to the iSCSI process. See Configure iSER with ESXi.

Establishing iSCSI Connections

In the ESXi context, the term target identifies a single storage unit that your host can access. The terms storage device and LUN describe a logical volume that represents storage space on a target. Typically, the terms device and LUN, in the ESXi context, mean a SCSI volume presented to your host from a storage target and available for formatting.

Different iSCSI storage vendors present storage to hosts in different ways. Some vendors present multiple LUNs on a single target. Others present multiple targets with one LUN each.

Figure 67: Target Compared to LUN Representations



In these examples, three LUNs are available in each of these configurations. In the first case, the host detects one target but that target has three LUNs that can be used. Each of the LUNs represents individual storage volume. In the second case, the host detects three different targets, each having one LUN.

Host-based iSCSI initiators establish connections to each target. Storage systems with a single target containing multiple LUNs have traffic to all the LUNs on a single connection. With a system that has three targets with one LUN each, the host uses separate connections to the three LUNs.

This information is useful when you are trying to aggregate storage traffic on multiple connections from the host with multiple iSCSI adapters. You can set the traffic for one target to a particular adapter, and use a different adapter for the traffic to another target.

iSCSI Storage System Types

ESXi supports different storage systems and arrays.

The types of storage that your host supports include active-active, active-passive, and ALUA-compliant.

Active-active storage system	Supports access to the LUNs simultaneously through all the storage ports that are available without significant performance degradation. All the paths are always active, unless a path fails.
Active-passive storage system	A system in which one storage processor is actively providing access to a given LUN. The other processors act as a backup for the LUN and can be actively providing access to other LUN I/O. I/O can be successfully sent only to an active port for a given LUN. If access through the active storage port fails, one of the passive storage processors can be activated by the servers accessing it.
Asymmetrical storage system	Supports Asymmetric Logical Unit Access (ALUA). ALUA-compliant storage systems provide different levels of access per

	port. With ALUA, hosts can determine the states of target ports and prioritize paths. The host uses some of the active paths as primary and others as secondary.
Virtual port storage system	Supports access to all available LUNs through a single virtual port. Virtual port storage systems are active-active storage devices, but hide their multiple connections though a single port. ESXi multipathing does not make multiple connections from a specific port to the storage by default. Some storage vendors supply session managers to establish and manage multiple connections to their storage. These storage systems handle port failovers and connection balancing transparently. This capability is often called transparent failover.

Discovery, Authentication, and Access Control

You can use several mechanisms to discover your storage and to limit access to it.

You must configure your host and the iSCSI storage system to support your storage access control policy.

Discovery

A discovery session is part of the iSCSI protocol. It returns the set of targets you can access on an iSCSI storage system. The two types of discovery available on ESXi are dynamic and static. Dynamic discovery obtains a list of accessible targets from the iSCSI storage system. Static discovery can access only a particular target by target name and address.

For more information, see Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host.

Authentication

iSCSI storage systems authenticate an initiator by a name and key pair. ESXi supports the CHAP authentication protocol. To use CHAP authentication, the ESXi host and the iSCSI storage system must have CHAP enabled and have common credentials.

For information on enabling CHAP, see Configuring CHAP Parameters for iSCSI or iSER Storage Adapters.

Access Control

Access control is a policy set up on the iSCSI storage system. Most implementations support one or more of three types of access control:

- By initiator name
- By IP address
- By the CHAP protocol

Only initiators that meet all rules can access the iSCSI volume.

Using only CHAP for access control can slow down rescans because the ESXi host can discover all targets, but then fails at the authentication step. iSCSI rescans work faster if the host discovers only the targets it can authenticate.

How Virtual Machines Access Data on an iSCSI SAN

ESXi stores a virtual machine's disk files within a VMFS datastore that resides on a SAN storage device. When virtual machine guest operating systems send SCSI commands to their virtual disks, the SCSI virtualization layer translates these commands to VMFS file operations.

When a virtual machine interacts with its virtual disk stored on a SAN, the following process takes place:

1. When the guest operating system in a virtual machine reads or writes to SCSI disk, it sends SCSI commands to the virtual disk.
2. Device drivers in the virtual machine's operating system communicate with the virtual SCSI controllers.
3. The virtual SCSI controller forwards the commands to the VMkernel.
4. The VMkernel performs the following tasks.
   a. Locates an appropriate virtual disk file in the VMFS volume.
   b. Maps the requests for the blocks on the virtual disk to blocks on the appropriate physical device.
   c. Sends the modified I/O request from the device driver in the VMkernel to the iSCSI initiator, hardware or software.
5. If the iSCSI initiator is a hardware iSCSI adapter, independent or dependent, the adapter performs the following tasks.
   a. Encapsulates I/O requests into iSCSI Protocol Data Units (PDUs).
   b. Encapsulates iSCSI PDUs into TCP/IP packets.
   c. Sends IP packets over Ethernet to the iSCSI storage system.
6. If the iSCSI initiator is a software iSCSI adapter, the following takes place.
   a. The iSCSI initiator encapsulates I/O requests into iSCSI PDUs.
   b. The initiator sends iSCSI PDUs through TCP/IP connections.
   c. The VMkernel TCP/IP stack relays TCP/IP packets to a physical NIC.
   d. The physical NIC sends IP packets over Ethernet to the iSCSI storage system.
7. Ethernet switches and routers on the network carry the request to the appropriate storage device.

Error Correction

To protect the integrity of iSCSI headers and data, the iSCSI protocol defines error correction methods known as header digests and data digests.

Both parameters are disabled by default, but you can enable them. These digests pertain to, respectively, the header and SCSI data being transferred between iSCSI initiators and targets, in both directions.

Header and data digests check the noncryptographic data integrity beyond the integrity checks that other networking layers, such as TCP and Ethernet, provide. The digests check the entire communication path, including all elements that can change the network-level traffic, such as routers, switches, and proxies.

The existence and type of the digests are negotiated when an iSCSI connection is established. When the initiator and target agree on a digest configuration, this digest must be used for all traffic between them.

Enabling header and data digests requires additional processing for both the initiator and the target, and can affect throughput and CPU use performance.

Note: Systems that use the Intel Nehalem processors offload the iSCSI digest calculations, as a result, reducing the impact on performance.

For information on enabling header and data digests, see Configuring Advanced Parameters for iSCSI.

Configuring iSCSI and iSER Adapters and Storage

Before ESXi can work with iSCSI SAN, you must set up your iSCSI environment.

The process of preparing your iSCSI environment involves the following steps:

Step	Details
Set up iSCSI storage	For information, see your storage vendor documentation. In addition, follow these recommendations:

Step	Details
	• ESXi iSCSI SAN Recommendations and Restrictions • Best Practices for iSCSI Storage
Configure iSCSI/iSER adapters	Use an appropriate workflow to configure your adapter: • Set Up Independent Hardware iSCSI Adapters • Configure Dependent Hardware iSCSI Adapters • Configure the Software iSCSI Adapter • Configure iSER with ESXi
Create a datastore on iSCSI storage	Creating Datastores

ESXi iSCSI SAN Recommendations and Restrictions

To work properly with iSCSI SAN, your ESXi environment must follow specific recommendations. In addition, several restrictions exist when you use ESXi with iSCSI SAN.

For additional information about using vSphere with iSCSI, see Best Practices For Running VMware vSphere On iSCSI blog.

iSCSI Storage Recommendations

- Verify that your ESXi host supports the iSCSI SAN storage hardware and firmware. For an up-to-date list, see *VMware Compatibility Guide*.
- To ensure that the host recognizes LUNs at startup time, configure all iSCSI storage targets so that your host can access them and use them. Configure your host so that it can discover all available iSCSI targets.
- Unless you are using diskless servers, set up a diagnostic partition on local storage. If you have diskless servers that boot from iSCSI SAN, see General Recommendations for Boot from iSCSI SAN for information about diagnostic partitions with iSCSI.
- Set the SCSI controller driver in the guest operating system to a large enough queue.
- VMtools increases the default disk timeout SCSI `TimeoutValue` parameter to 180 seconds. On virtual machines without VMtools, increase the value of the SCSI `TimeoutValue` parameter. With this parameter set up, the VMs can better tolerate delayed I/O resulting from a path failover. For information, see Set Timeout on Windows Guest OS or the KB 1009465.
- Configure your environment to have only one VMFS datastore for each LUN.

iSCSI Storage Restrictions

- ESXi does not support iSCSI-connected tape devices.
- You cannot use virtual-machine multipathing software to perform I/O load balancing to a single physical LUN.
- ESXi does not support multipathing when you combine independent hardware adapters with either software or dependent hardware adapters.

Configuring iSCSI Parameters for Adapters

Before your ESXi host can discover iSCSI storage, you must configure your iSCSI adapters. When you configure the adapters, you set several iSCSI parameters.

iSCSI Networking

For certain types of iSCSI adapters, you must configure VMkernel networking.

You can verify the network configuration by using the `vmkping` utility.

The independent hardware iSCSI adapter does not require VMkernel networking. You can configure network parameters, such as an IP address, subnet mask, and default gateway on the independent hardware iSCSI adapter.

All types of iSCSI adapters support IPv4 and IPv6 protocols.

iSCSI Adapter (vmhba)	Description	VMkernel Networking	Adapter Network Settings
Independent Hardware iSCSI Adapter	Third-party adapter that offloads the iSCSI and network processing and management from your host.	Not required.	For information, see Edit Network Settings for Hardware iSCSI.
Software iSCSI Adapter	Uses standard NICs to connect your host to a remote iSCSI target on the IP network.	Required. For information, see Setting Up Network for iSCSI and iSER.	N/A
Dependent Hardware iSCSI Adapter	Third-party adapter that depends on VMware networking and iSCSI configuration and management interfaces.	Required For information, see Setting Up Network for iSCSI and iSER.	N/A
VMware iSER Adapter	Uses an RDMA-capable network adapter to connect your host to a remote iSCSI target.	Required For information, see Setting Up Network for iSCSI and iSER.	N/A

Discovery Methods

For all types of iSCSI adapters, you must set the dynamic discovery address or static discovery address. In addition, you must provide a target name of the storage system. For software iSCSI and dependent hardware iSCSI, the address is pingable using `vmkping`.

See Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host.

CHAP Authentication

Enable the CHAP parameter on the initiator and the storage system side. After authentication is enabled, it applies to all targets that are not yet discovered. It does not apply to targets that are already discovered.

See Configuring CHAP Parameters for iSCSI or iSER Storage Adapters.

Set Up Independent Hardware iSCSI Adapters

An independent hardware iSCSI adapter is a specialized third-party adapter capable of accessing iSCSI storage over TCP/IP. This iSCSI adapter handles all iSCSI and network processing and management for your ESXi system.

- Verify whether the adapter must be licensed.
- Install the adapter on your ESXi host.

For information about licensing, installation, and firmware updates, see vendor documentation.

The process of setting up the independent hardware iSCSI adapter includes these steps.

Step	Description
View Independent Hardware iSCSI Adapters	View an independent hardware iSCSI adapter and verify that it is correctly installed and ready for configuration.
Modify General Properties for iSCSI or iSER Adapters	If needed, change the default iSCSI name and alias assigned to your iSCSI adapters. For the independent hardware iSCSI adapters, you can also change the default IP settings.
Edit Network Settings for Hardware iSCSI	Change default network settings so that the adapter is configured properly for the iSCSI SAN.
Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host	Set up dynamic discovery. With dynamic discovery, each time the initiator contacts a specified iSCSI storage system, it sends the SendTargets request to the system. The iSCSI system responds by supplying a list of available targets to the initiator. In addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets.
Set Up CHAP for iSCSI or iSER Storage Adapter	If your iSCSI environment uses the Challenge Handshake Authentication Protocol (CHAP), configure it for your adapter.
Enable Jumbo Frames for Independent Hardware iSCSI	If your iSCSI environment supports Jumbo Frames, enable them for the adapter.

View Independent Hardware iSCSI Adapters

On the ESXi host, view an independent hardware iSCSI adapter and verify that it is correctly installed and ready for configuration.

Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

After you install an independent hardware iSCSI adapter on the host, it appears on the list of storage adapters available for configuration. You can view its properties.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**.
   If installed, the hardware iSCSI adapter appears on the list of storage adapters.
4. Select the adapter to view.
   The default details for the adapter appear.

Adapter Information	Description
Model	Model of the adapter.
iSCSI Name	Unique name formed according to iSCSI standards that identifies the iSCSI adapter. You can edit the iSCSI name.
iSCSI Alias	A friendly name used instead of the iSCSI name. You can edit the iSCSI alias.
IP Address	Address assigned to the iSCSI HBA.
Targets	Number of targets accessed through the adapter.
Devices	All storage devices or LUNs the adapter can access.
Paths	All paths the adapter uses to access storage devices.

Edit Network Settings for Hardware iSCSI

After you install an independent hardware iSCSI adapter on an ESXi host, you might need to change its default network settings so that the adapter is configured properly for the iSCSI SAN.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
4. Click the **Network Settings** tab and click **Edit**.
5. In the IPv4 settings section, disable IPv6 or select the method to obtain IP addresses.

   Note: The automatic DHCP option and static option are mutually exclusive.

Option	Description
No IPv4 settings	Disable IPv4.
Obtain IPv4 settings automatically	Use DHCP to obtain IP settings.
Use static IPv4 settings	Enter the IPv4 IP address, subnet mask, and default gateway for the iSCSI adapter.

6. In the IPv6 settings section, disable IPv6 or select an appropriate option for obtaining IPv6 addresses.

   Note: Automatic options and the static option are mutually exclusive.

Option	Description
No IPv6 settings	Disable IPv6.
Enable IPv6	Select an option for obtaining IPv6 addresses.
Obtain IPv6 addresses automatically through DHCP	Use DHCP to obtain IPv6 addresses.
Obtain IPv6 addresses automatically through Router Advertisement	Use router advertisement to obtain IPv6 addresses.
Override Link-local address for IPv6	Override the link-local IP address by configuring a static IP address.
Static IPv6 addresses	1. Click **Add** to add a new IPv6 address. 2. Enter the IPv6 address and subnet prefix length, and click **OK**.

7. In the DNS settings section, provide IP addresses for a preferred DNS server and an alternate DNS server.
   You must provide both values.

Configure Dependent Hardware iSCSI Adapters

A dependent hardware iSCSI adapter is a third-party adapter that depends on VMware networking, and iSCSI configuration and management interfaces provided by VMware.

An example of a dependent iSCSI adapter is a Broadcom 5709 NIC. When installed on a host, it presents its two components, a standard network adapter and an iSCSI engine, to the same port. The iSCSI engine appears on the list of storage adapters as an iSCSI adapter (vmhba).

The iSCSI adapter is enabled by default. To make it functional, you must connect it, through a virtual VMkernel adapter (vmk), to a physical network adapter (vmnic) associated with it. You can then configure the iSCSI adapter.

After you configure the dependent hardware iSCSI adapter, the discovery and authentication data is passed through the network connection. The iSCSI traffic goes through the iSCSI engine, bypassing the network.

The entire setup and configuration process for the dependent hardware iSCSI adapters involves several steps.

Step	Description
View Dependent Hardware iSCSI Adapters	View a dependent hardware iSCSI adapter to verify that it is correctly loaded.
Modify General Properties for iSCSI or iSER Adapters	If needed, change the default iSCSI name and alias assigned to your adapter.
Determine Association Between iSCSI and Network Adapters	You must create network connections to bind dependent iSCSI and physical network adapters. To create the connections correctly, determine the name of the physical NIC with which the dependent hardware iSCSI adapter is associated.
Configure Port Binding for iSCSI or iSER	Configure connections for the traffic between the iSCSI component and the physical network adapters. The process of configuring these connections is called port binding.
Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host	Set up dynamic discovery. With dynamic discovery, each time the initiator contacts a specified iSCSI storage system, it sends the SendTargets request to the system. The iSCSI system responds by supplying a list of available targets to the initiator. In addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets.
Set Up CHAP for iSCSI or iSER Storage Adapter	If your iSCSI environment uses the Challenge Handshake Authentication Protocol (CHAP), configure it for your adapter.
Set Up CHAP for Target	You can also configure different CHAP credentials for each discovery address or static target.
Enable Jumbo Frames for Networking	If your iSCSI environment supports Jumbo Frames, enable them for the adapter.

Dependent Hardware iSCSI Considerations

When you use dependent hardware iSCSI adapters with ESXi, certain considerations apply.

- When you use any dependent hardware iSCSI adapter, performance reporting for a NIC associated with the adapter might show little or no activity, even when iSCSI traffic is heavy. This behavior occurs because the iSCSI traffic bypasses the regular networking stack.
- If you use a third-party virtual switch, for example Cisco Nexus 1000V DVS, disable automatic pinning. Use manual pinning instead, making sure to connect a VMkernel adapter (vmk) to an appropriate physical NIC (vmnic). For information, refer to your virtual switch vendor documentation.
- The Broadcom iSCSI adapter performs data reassembly in hardware, which has a limited buffer space. When you use the Broadcom iSCSI adapter in a congested network or under heavy load, enable flow control to avoid performance degradation.

  Flow control manages the rate of data transmission between two nodes to prevent a fast sender from overrunning a slow receiver. For best results, enable flow control at the end points of the I/O path, at the hosts and iSCSI storage systems.

  To enable flow control for the host, use the `esxcli system module parameters` command.
- Dependent hardware adapters support IPv4 and IPv6.

View Dependent Hardware iSCSI Adapters

On an ESXi host, view a dependent hardware iSCSI adapter to verify that it is correctly loaded.

If installed, the dependent hardware iSCSI adapter (vmhba#) appears on the list of storage adapters under such category as, for example, Broadcom iSCSI Adapter. If the dependent hardware adapter does not appear on the list of storage adapters, check whether it needs to be licensed. See your vendor documentation.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**.
4. Select the adapter (vmhba#) to view.

   The default details for the adapter appear, including the iSCSI name, iSCSI alias, and the status.

Although the dependent iSCSI adapter is enabled by default, to make it functional, you must set up networking for the iSCSI traffic and bind the adapter to the appropriate VMkernel iSCSI port. You then configure discovery addresses and CHAP parameters.

Determine Association Between iSCSI and Network Adapters

On an ESXi host, network connections bind dependent iSCSI and physical network adapters. To create the connections correctly, you must determine the name of the physical NIC with which the dependent hardware iSCSI adapter is associated.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**.
4. Select the iSCSI adapter (vmhba#) and click the **Network Port Binding** tab under adapter details.
5. Click **Add**.

   The network adapter (vmnic#) that corresponds to the dependent iSCSI adapter is listed in the Physical Network Adapter column.

If the VMkernel Adapter column is empty, create a VMkernel adapter (vmk#) for the physical network adapter (vmnic#) and then bind them to the associated dependent hardware iSCSI. See Setting Up Network for iSCSI and iSER.

Configure the Software iSCSI Adapter

With the software-based iSCSI implementation, you can use standard NICs to connect your host to a remote iSCSI target on the IP network. The software iSCSI adapter that is built into ESXi facilitates this connection by communicating with the physical NICs through the network stack.

When you use the software iSCSI adapters, consider the following:

- Designate a separate network adapter for iSCSI. Do not use iSCSI on 100 Mbps or slower adapters.
- Avoid hard coding the name of the software adapter, vmhbaXX, in the scripts. It is possible for the name to change from one ESXi release to another. The change might cause failures of your existing scripts if they use the hardcoded old name. The name change does not affect the behavior of the iSCSI software adapter.

The process of configuring the software iSCSI adapter involves several steps.

Step	Description
Activate or Disable the Software iSCSI Adapter	Activate your software iSCSI adapter so that your host can use it to access iSCSI storage.

Step	Description
Modify General Properties for iSCSI or iSER Adapters	If needed, change the default iSCSI name and alias assigned to your adapter.
Configure Port Binding for iSCSI or iSER	Configure connections for the traffic between the iSCSI component and the physical network adapters. The process of configuring these connections is called port binding.
Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host	Set up dynamic discovery. With dynamic discovery, each time the initiator contacts a specified iSCSI storage system, it sends the SendTargets request to the system. The iSCSI system responds by supplying a list of available targets to the initiator. In addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets.
Set Up CHAP for iSCSI or iSER Storage Adapter	If your iSCSI environment uses the Challenge Handshake Authentication Protocol (CHAP), configure it for your adapter.
Set Up CHAP for Target	You can also configure different CHAP credentials for each discovery address or static target.
Enable Jumbo Frames for Networking	If your iSCSI environment supports Jumbo Frames, enable them for the adapter.

Activate or Disable the Software iSCSI Adapter

You must activate your software iSCSI adapter so that your ESXi host can use it to access iSCSI storage. If you do not need the software iSCSI adapter after activation, you can disable it.

Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

Note: If you boot from iSCSI using the software iSCSI adapter, the adapter is enabled and the network configuration is created at the first boot. If you disable the adapter, it is reenabled each time you boot the host.

You can activate only one software iSCSI adapter.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Enable or disable the adapter.

Option	Description
Enable the software iSCSI adapter	1. Under **Storage**, click **Storage Adapters**, and click the **Add** icon. 2. Select **Software iSCSI Adapter** and confirm that you want to add the adapter. The software iSCSI adapter (vmhba#) is enabled and appears on the list of storage adapters. After enabling the adapter, the host assigns the default iSCSI name to it. You can now complete the adapter configuration.
Disable the software iSCSI adapter	1. Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to disable. 2. Click the **Properties** tab. 3. Click **Disable** and confirm that you want to disable the adapter. The status indicates that the adapter is disabled.

Option	Description
	4. Reboot the host. After the reboot, the adapter no longer appears on the list of storage adapters. The storage devices associated with the adapter become inaccessible. You can later activate the adapter.

Configure iSER with ESXi

In addition to traditional iSCSI, ESXi supports the iSCSI Extensions for RDMA (iSER) protocol. When the iSER protocol is enabled, the iSCSI framework on the ESXi host can use the Remote Direct Memory Access (RDMA) transport instead of TCP/IP. You can configure iSER on your ESXi host.

For more information about the iSER protocol, see Using iSER Protocol with ESXi.

The entire setup and configuration process for VMware iSER involves several steps.

Step	Description
Install and View an RDMA Capable Network Adapter	To configure iSER with ESXi, you must first install an RDMA capable network adapter, for example, Mellanox Technologies MT27700 Family ConnectX-4. After you install this type of adapter, the vSphere Client displays its two components, an RDMA adapter and a physical network adapter `vmnic#`.
Enable the VMware iSER Adapter	To be able to use the RDMA capable adapter for iSCSI, use the `esxcli` to enable the VMware iSER storage component. The component appears in the vSphere Client as a `vmhba#` storage adapter under the VMware iSCSI over RDMA (iSER) Adapter category.
Modify General Properties for iSCSI or iSER Adapters	If needed, change the default name and alias assigned to the iSER storage adapter `vmhba#`.
Configure Port Binding for iSCSI or iSER	You must create network connections to bind the iSER storage adapter `vmhba#` and the RDMA capable network adapter `vmnic#`. The process of configuring these connections is called port binding. **Note:** iSER does not support NIC teaming. When configuring port binding, use only one RDMA adapter per vSwitch.
Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host	Set up the dynamic or static discovery for your iSER storage adapter `vmhba#`. With the dynamic discovery, each time the initiator contacts a specified iSER storage system, it sends the SendTargets request to the system. The iSER system responds by supplying a list of available targets to the initiator. With the static discovery, you manually enter information for the targets.
Set Up CHAP for iSCSI or iSER Storage Adapter	If your environment uses the Challenge Handshake Authentication Protocol (CHAP), configure it for your iSER storage adapter `vmhba#`.
Set Up CHAP for Target	You can also configure different CHAP credentials for each discovery address or static target.
Enable Jumbo Frames for Networking	If your environment supports Jumbo Frames, enable them for the iSER storage adapter `vmhba#`.

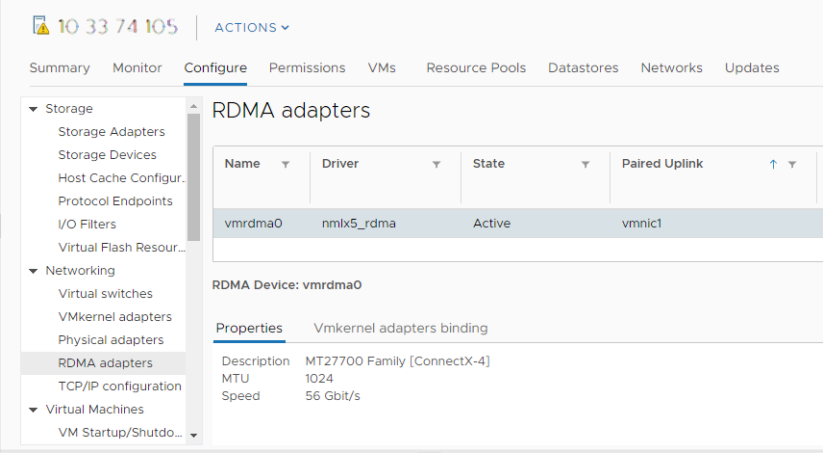
Install and View an RDMA Capable Network Adapter

ESXi supports RDMA capable network adapters, for example, Mellanox Technologies MT27700 Family ConnectX-4. After you install such adapter on your host, the vSphere Client displays its two components, an RDMA adapter and a physical network adapter.

You can use the vSphere Client to view the RDMA adapter and its corresponding network adapter.

1. In the vSphere Client, navigate to the ESXi host.
2. Under **Networking**, click **RDMA adapters**.

   In this example, the RDMA adapter appears on the list as `vmrdma0`. The **Paired Uplink** column displays the network component as the `vmnic1` physical network adapter.



3. To verify the description of the adapter, select the RDMA adapter from the list, and click the **Properties** tab.

You can use the `vmnic#` network component of the adapter for such storage configurations as iSER or NVMe over RDMA. For the iSER configuration steps, see Configure iSER with ESXi. For information about NVMe over RDMA, see Configure Adapters for NVMe over RDMA (RoCE v2) Storage.

Enable the VMware iSER Adapter

To be able to use the RDMA capable adapter for iSCSI, use the `esxcli` to enable the VMware iSER storage component. After you enable the component, it appears in the vSphere Client as a `vmhba#` storage adapter under the VMware iSCSI over RDMA (iSER) Adapter category.

- Make sure that your iSCSI storage supports the iSER protocol.
- Install the RDMA capable adapter on your ESXi host. For information, see Install and View an RDMA Capable Network Adapter.
- For RDMA capable adapters that support RDMA over Converged Ethernet (RoCE), determine the RoCE version that the adapter uses.
- Use the RDMA capable switch.
- Enable flow control on the ESXi host. To enable flow control for the host, use the `esxcli system module parameters` command.
- Make sure to configure RDMA switch ports to create lossless connections between the iSER initiator and target.

1. Use the ESXi Shell or vSphere CLI to enable the VMware iSER storage adapter and set its RoCE version.
   a) Enable the iSER storage adapter.

      ```
      esxcli rdma iser add
      ```

b) Verify that the iSER adapter has been added.

```
esxcli iscsi adapter list
```

The output is similar to the following.

```
Adapter Driver State UID Description
------- ------ ------- ------------- -----------------------------------
vmhba64 iser unbound iscsi.vmhba64 VMware iSCSI over RDMA (iSER) Adapter
```

c) Specify the RoCE version that iSER uses to connect to the target.

Use the RoCE version of the RDMA capable adapter. The command you enter is similar to the following:

```
esxcli rdma iser params set -a vmhba64 -r 1
```

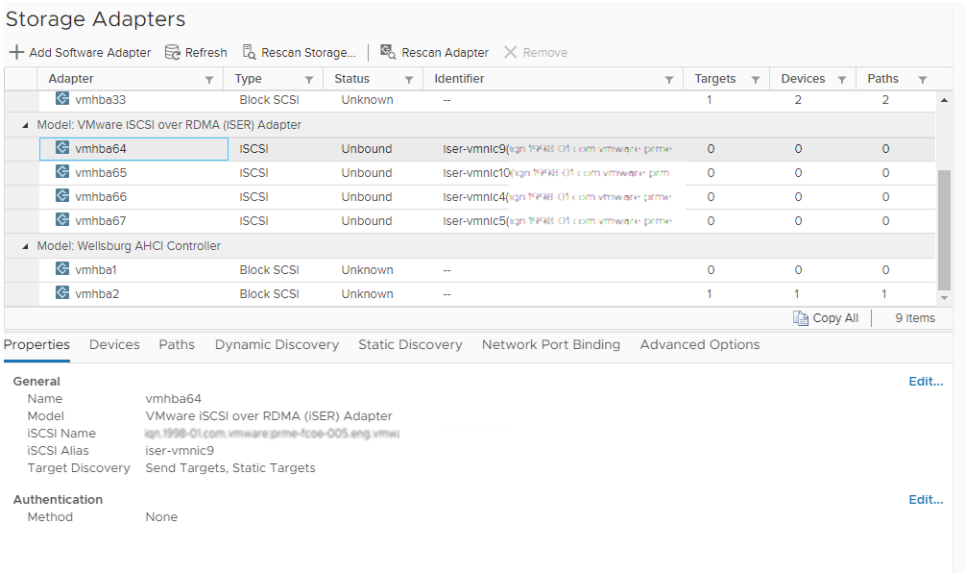
When the command completes, a message similar to the following appears in the VMkernel log.

```
vmkernel.0:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce: Setting roce type:
 1 for vmhba: vmhba64
vmkernel.0:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce: Setting rdma port:
 3260 for vmhba: vmhba64
```

If you do not specify the RoCE version, the host defaults to the highest RoCE version the RDMA capable adapter supports.

2. Use the vSphere Client to display the iSER adapter.
   a) In the vSphere Client, navigate to the ESXi host.
   b) Click the **Configure** tab.
   c) Under **Storage**, click **Storage Adapters**, and review the list of adapters.

   If you enabled the adapter, it appears as a storage `vmhba#` adapter on the list under the VMware iSCSI over RDMA (iSER) Adapter category.



3. Select the iSER storage `vmhba#` to review its properties or perform the following tasks.

Option	Description
Configure port binding for the iSER storage adapter	You must create network connections to bind the iSER storage adapter `vmhba#` and the RDMA capable network adapter `vmnic#`. The process of configuring these connections is called

Option	Description
	port binding. For general information about port binding, see Setting Up Network for iSCSI and iSER. To configure port binding for iSER, see Configure Port Binding for iSCSI or iSER.
Set up dynamic or static discovery for the iSER storage adapter	For information, see Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host.
Configure the Challenge Handshake Authentication Protocol (CHAP) for the iSER storage adapter	For information, see Set Up CHAP for iSCSI or iSER Storage Adapter.

Modify General Properties for iSCSI or iSER Adapters

You can change default name and alias assigned to your iSCSI or iSER storage adapters by the ESXi host. For the independent hardware iSCSI adapters, you can also change the default IP settings.

Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

Important: When you modify any default properties for your adapters, make sure to use correct formats for their names and IP addresses.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
4. Click the **Properties** tab, and click **Edit** in the General panel.
5. Optional: Modify the following general properties.

Option	Description
iSCSI Name	Unique name formed according to iSCSI standards that identifies the iSCSI adapter. If you change the name, make sure that the name you enter is worldwide unique and properly formatted. Otherwise, certain storage devices might not recognize the iSCSI adapter.
iSCSI Alias	A friendly name you use instead of the iSCSI name.

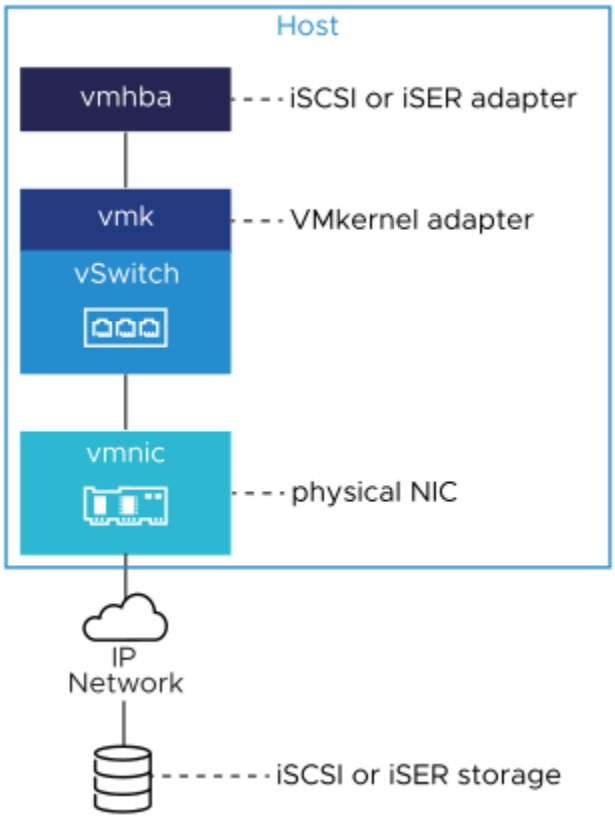
If you change the iSCSI name, it is used for new iSCSI sessions. For existing sessions, the new settings are not used until you log out and log in again.
For other configuration steps you can perform for the iSCSI or iSER storage adapters, see the following topics:

- Set Up Independent Hardware iSCSI Adapters
- Configure Dependent Hardware iSCSI Adapters
- Configure the Software iSCSI Adapter
- Configure iSER with ESXi

Setting Up Network for iSCSI and iSER

Certain types of iSCSI adapters depend on the VMkernel networking. These adapters include the software or dependent hardware iSCSI adapters, and the VMware iSCSI over RDMA (iSER) adapter. If your environment includes any of these adapters, you must configure connections for the traffic between the iSCSI or iSER component and the physical network adapters.

Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter. You then associate the VMkernel adapter with an appropriate iSCSI or iSER adapter. This process is called port binding.



Follow these rules when configuring the port binding:

- You can connect the software iSCSI adapter with any physical NICs available on your host.
- The dependent iSCSI adapters must be connected only to their own physical NICs.
- You must connect the iSER adapter only to the RDMA-capable network adapter.

For specific considerations on when and how to use network connections with software iSCSI, see the VMware knowledge base article at http://kb.vmware.com/kb/2038869.

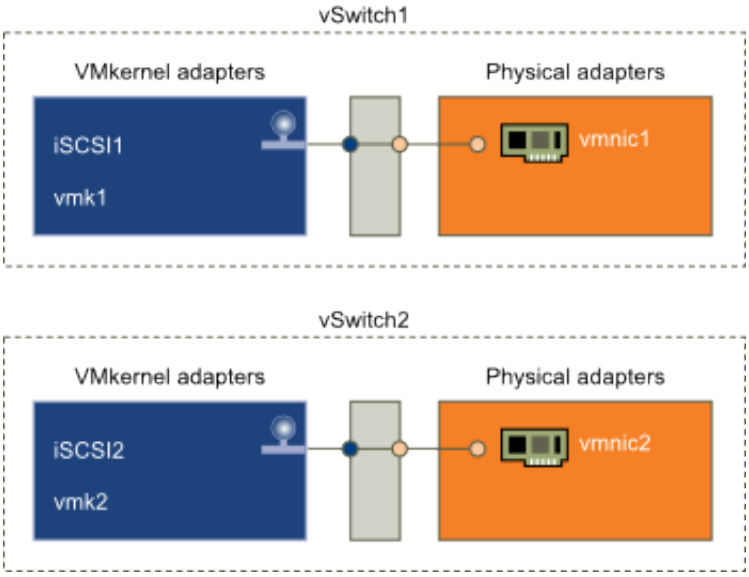
Multiple Network Adapters in iSCSI or iSER Configuration

If your host has more than one physical network adapter for iSCSI or iSER, you can use the adapters for multipathing.

You can use multiple physical adapters in a single or multiple switch configurations.

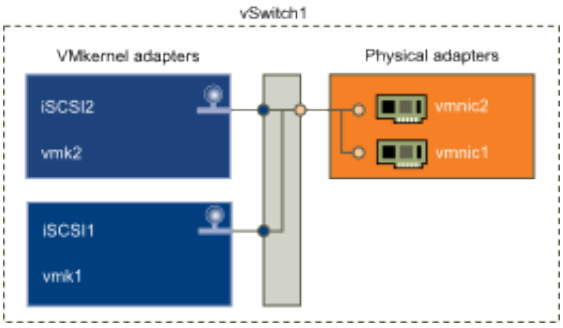
In the multiple switch configuration, you designate a separate vSphere switch for each virtual-to-physical adapter pair.

Figure 68: 1:1 Adapter Mapping on Separate vSphere Standard Switches



An alternative is to add all NICs and VMkernel adapters to the single vSphere switch. The number of VMkernel adapters must correspond to the number of physical adapters on the vSphere Standard switch. The single switch configuration is not appropriate for iSER because iSER does not support NIC teaming.

Figure 69: 1:1 Adapter Mapping on a Single vSphere Standard Switch



For that type of configuration, you must override the default network setup and make sure that each VMkernel adapter maps to only one corresponding active physical adapter, as the table indicates.

VMkernel Adapter (vmk#)	Physical Network Adapter (vmnic#)
vmk1 (iSCSI1)	**Active Adapters** vmnic1 **Unused Adapters** vmnic2
vmk2 (iSCSI2)	**Active Adapters** vmnic2 **Unused Adapters** vmnic1

You can also use distributed switches. For more information about vSphere distributed switches and how to change the default network policy, see the *vSphere Networking* documentation.

The following considerations apply when you use multiple physical adapters:

- Physical network adapters must be on the same subnet as the storage system they connect to.
- (Applies only to iSCSI and not to iSER) If you use separate vSphere switches, you must connect them to different IP subnets. Otherwise, VMkernel adapters might experience connectivity problems and the host fails to discover the LUNs.
- The single switch configuration is not appropriate for iSER because iSER does not support NIC teaming.

Do not use port binding when any of the following conditions exist:

- Array target iSCSI ports are in a different broadcast domain and IP subnet.
- VMkernel adapters used for iSCSI connectivity exist in different broadcast domains, IP subnets, or use different virtual switches.

  Note: In iSER configurations, the VMkernel adapters used for iSER connectivity cannot be used for converged traffic. The VMkernel adapters that you created to enable connectivity between the ESXi host with iSER and the iSER target must be used only for iSER traffic.

Best Practices for Configuring Networking with Software iSCSI

When you configure networking with software iSCSI, consider several best practices.

Software iSCSI Port Binding

You can bind the software iSCSI initiator on the ESXi host to a single or multiple VMkernel ports, so that iSCSI traffic flows only through the bound ports. Unbound ports are not used for iSCSI traffic.

When port binding is configured, the iSCSI initiator creates iSCSI sessions from all bound ports to all configured target portals.

See the following examples.

VMkernel Ports	Target Portals	iSCSI Sessions
2 bound VMkernel ports	2 target portals	4 sessions (2 x 2)
4 bound VMkernel ports	1 target portal	4 sessions (4 x 1)
2 bound VMkernel ports	4 target portals	8 sessions (2 x 4)

Note: Make sure that all target portals are reachable from all VMkernel ports when port binding is used. Otherwise, iSCSI sessions might fail to create. As a result, the rescan operation might take longer than expected.

No Port Binding

If you do not use port binding, the ESXi networking layer selects the best VMkernel port based on its routing table. The host uses the port to create an iSCSI session with the target portal. Without the port binding, only one session per each target portal is created.

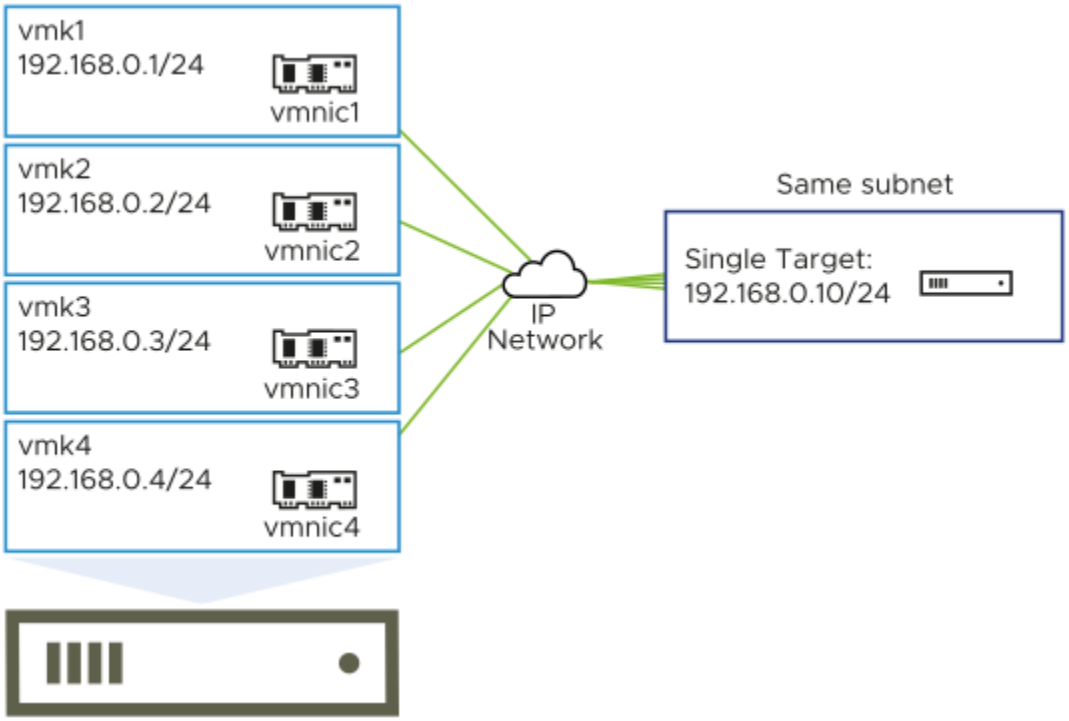
See the following examples.

VMkernel Ports	Target Portals	iSCSI Sessions
2 unbound VMkernel ports	2 target portals	2 sessions
4 unbound VMkernel ports	1 target portal	1 session
2 unbound VMkernel ports	4 target portals	4 sessions

Software iSCSI Multipathing

Example 1. Multiple paths for an iSCSI target with a single network portal

If your target has only one network portal, you can create multiple paths to the target by adding multiple VMkernel ports on your ESXi host and binding them to the iSCSI initiator.

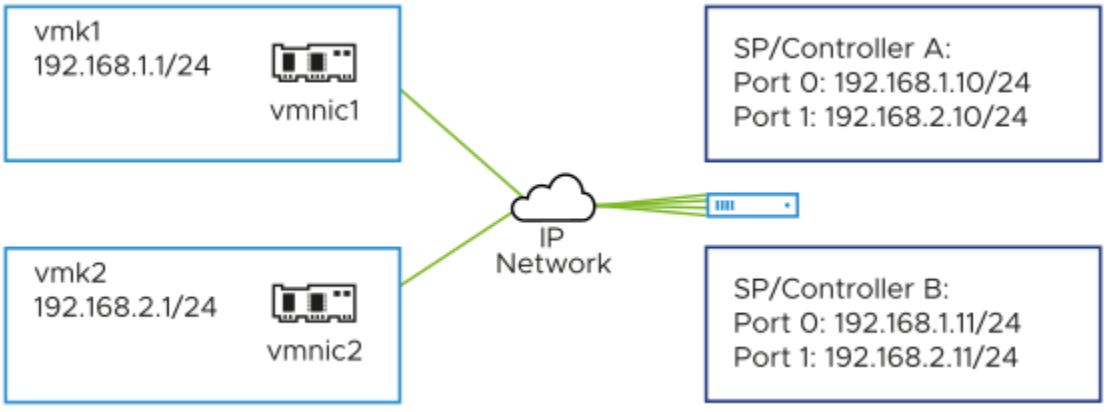


In this example, all initiator ports and the target portal are configured in the same subnet. The target is reachable through all bound ports. You have four VMkernel ports and one target portal, so total of four paths are created.

Without the port binding, only one path is created.

Example 2. Multiple paths with VMkernel ports in different subnets

You can create multiple paths by configuring multiple ports and target portals on different IP subnets. By keeping initiator and target ports in different subnets, you can force ESXi to create paths through specific ports. In this configuration, you do not use port binding because port binding requires that all initiator and target ports are on the same subnet.



ESXi selects vmk1 when connecting to Port 0 of Controller A and Controller B because all three ports are on the same subnet. Similarly, vmk2 is selected when connecting to Port 1 of Controller A and B. You can use NIC teaming in this configuration.

Total of four paths are created.

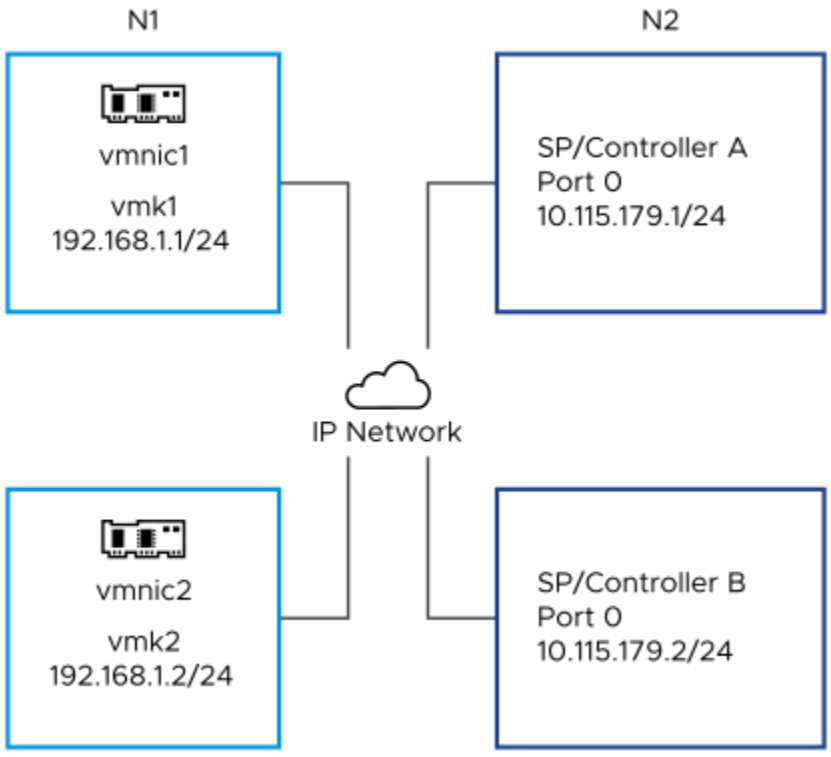
Paths	Description
Path 1	vmk1 and Port0 of Controller A
Path 2	vmk1 and Port0 of Controller B
Path 3	vmk2 and Port1 of Controller A
Path 4	vmk2 and Port1 of Controller B

Routing with Software iSCSI

You can use the `esxcli` command to add static routes for your iSCSI traffic. After you configure static routes, initiator and target ports in different subnets can communicate with each other.

Example 1. Using static routes with port binding

In this example, you keep all bound VMkernel ports in one subnet (N1) and configure all target portals in another subnet (N2). You can then add a static route for the target subnet (N2).

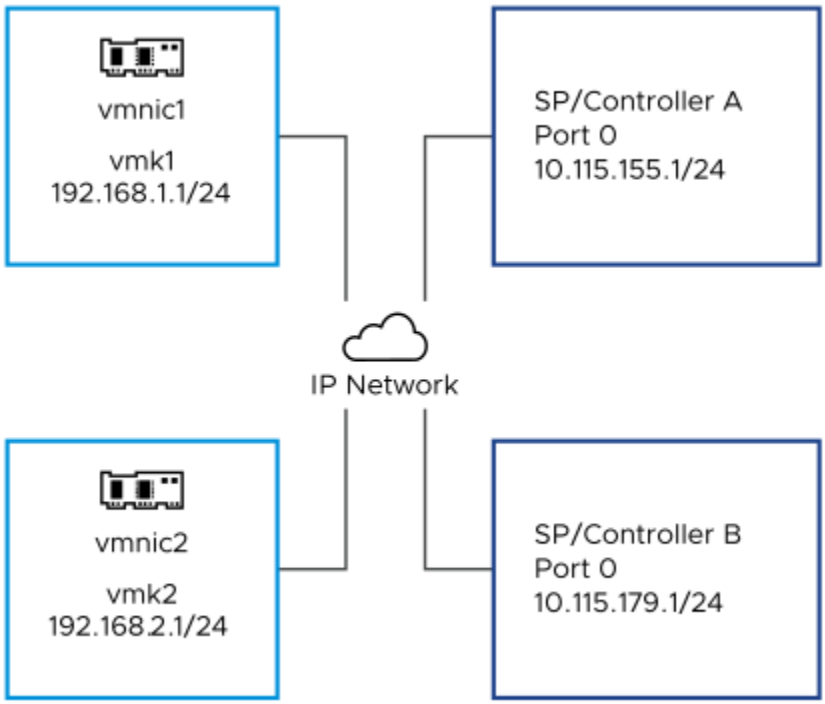


Use the following command:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.179.0/24
```

Example 2. Using static routes to create multiple paths

In this configuration, you use static routing when using different subnets. You cannot use the port binding with this configuration.



You configure vmk1 and vmk2 in separate subnets, 192.168.1.0 and 192.168.2.0. Your target portals are also in separate subnets, 10.115.155.0 and 10.155.179.0.

You can add the static route for 10.115.155.0 from vmk1. Make sure that the gateway is reachable from vmk1.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24
```

You then add static route for 10.115.179.0 from vmk2. Make sure that the gateway is reachable from vmk2.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24
```

When connecting with Port 0 of Controller A, vmk1 is used.

When connecting with Port 0 of Controller B, vmk2 is used.

Example 3. Routing with a separate gateway per vmkernel port

Starting with vSphere 6.5, you can configure a separate gateway per VMkernel port. If you use DHCP to obtain IP configuration for a VMkernel port, gateway information can also be obtained using DHCP.

To see gateway information per VMkernel port, use the following command:

```
# esxcli network ip interface ipv4 address list
 Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
 ----  --------------  -------------  --------------  ------------  --------------  --------
 vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
 vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
 vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

With separate gateways per VMkernel port, you use port binding to reach targets in different subnets.

Configure Port Binding for iSCSI or iSER

The port binding creates connections for the traffic between certain types of iSCSI and iSER adapters and the physical network adapters.

The following types of adapters require the port binding:

- Software iSCSI adapter
- Dependent hardware iSCSI adapter
- VMware iSCSI over RDMA (iSER) adapter

The following tasks discuss the network configuration with a vSphere Standard switch and a single physical network adapter. If you have multiple network adapters, see Multiple Network Adapters in iSCSI or iSER Configuration.

Note: iSER does not support NIC teaming. When configuring port binding for iSER, use only one RDMA-enabled physical adapter (vmnic#) and one VMkernel adapter (vmk#) per vSwitch.

You can also use the VMware vSphere®Distributed Switch™ and VMware NSX®Virtual Switch™ in the port binding configuration. For information about NSX virtual switches, see the *VMware NSX Data Center for vSphere* documentation.

If you use a vSphere distributed switch with multiple uplink ports, for port binding, create a separate distributed port group per each physical NIC. Then set the team policy so that each distributed port group has only one active uplink port. For detailed information on distributed switches, see the *vSphere Networking* documentation.

For other configuration steps you can perform for the iSCSI or iSER storage adapters, see the following topics:

- Configure Dependent Hardware iSCSI Adapters
- Configure the Software iSCSI Adapter
- Configure iSER with ESXi

Create a Single VMkernel Adapter for iSCSI or iSER

Connect the VMkernel, which runs services for iSCSI storage, to a physical network adapter on your ESXi host. You then use the created VMkernel adapter in the port binding configuration with the iSCSI or iSER adapters.

- If you are creating a VMkernel adapter for dependent hardware iSCSI, you must use the physical network adapter (vmnic#) that corresponds to the iSCSI component. See Determine Association Between iSCSI and Network Adapters.
- With the iSER adapter, make sure to use an appropriate RDMA-capable vmnic#. See Install and View an RDMA Capable Network Adapter.

The following types of adapters require the port binding:

- Software iSCSI adapter
- Dependent hardware iSCSI adapter
- VMware iSCSI over RDMA (iSER) adapter

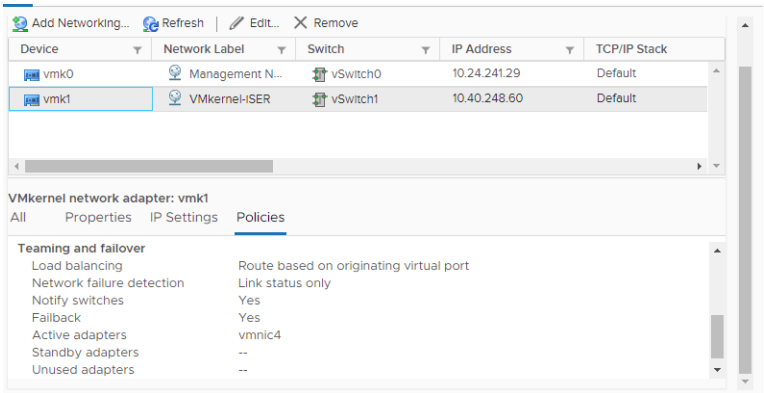
1. In the vSphere Client, navigate to the ESXi host.
2. Select **Add Networking** from the right-click menu.
3. Select **VMkernel Network Adapter**, and click **Next**.
4. Select **New standard switch** to create a vSphere Standard switch.
5. Click the **Add adapters** icon, and select an appropriate network adapter (vmnic#) to use for iSCSI.

   Make sure to assign the adapter to Active Adapters.
6. Enter a network label.

   A network label is a friendly name that identifies the VMkernel adapter that you are creating, for example, iSCSI or iSER.

7. Specify the IP settings.
8. Review the information and click **Finish**.

   You created the virtual VMkernel adapter (vmk#) for a physical network adapter (vmnic#) on your host.
9. Verify your configuration.
   a) Under **Networking**, select **VMkernel Adapters**, and select the VMkernel adapter (vmk#) from the list.
   b) Click the **Policies** tab, and verify that the corresponding physical network adapter (vmnic#) appears as an active adapter under **Teaming and failover**.



If your host has one physical network adapter for iSCSI traffic, bind the VMkernel adapter that you created to the iSCSI or iSER vmhba adapter.

If you have multiple network adapters, you can create additional VMkernel adapters and then perform iSCSI binding. The number of virtual adapters must correspond to the number of physical adapters on the host. For information, see Multiple Network Adapters in iSCSI or iSER Configuration.

Bind iSCSI or iSER Adapters to VMkernel Adapters

On the ESXi host, bind an iSCSI or iSER adapter with a VMkernel adapter.

Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.
Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

The following types of adapters require the port binding:

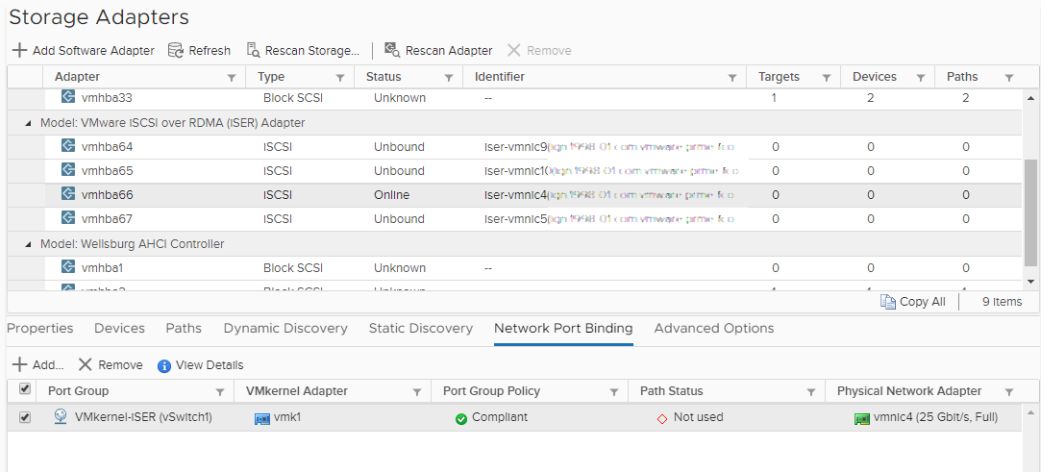
- Software iSCSI adapter
- Dependent hardware iSCSI adapter
- VMware iSCSI over RDMA (iSER) adapter

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the appropriate iSCSI or iSER adapter (vmhba#) from the list.
4. Click the **Network Port Binding** tab and click the **Add** icon.
5. Select a VMkernel adapter to bind with the iSCSI or iSER adapter.

   Note: Make sure that the network policy for the VMkernel adapter is compliant with the binding requirements.

   You can bind the software iSCSI adapter to one or more VMkernel adapters. For a dependent hardware iSCSI adapter or the iSER adapter, only one VMkernel adapter associated with the correct physical NIC is available.

6. Click **OK**.
   The network connection appears on the list of network port bindings for the iSCSI or iSER adapter.



Review Port Binding Details on the ESXi Host

Review networking details of the VMkernel adapter that is bound to the iSCSI or iSER vmhba adapter.

The following types of adapters require the port binding:

- Software iSCSI adapter
- Dependent hardware iSCSI adapter
- VMware iSCSI over RDMA (iSER) adapter

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the appropriate iSCSI or iSER adapter from the list.
4. Click the **Network Port Binding** tab and select the VMkernel adapter from the list.
5. Click the **View Details** icon.
6. Review the VMkernel adapter and physical adapter information by switching between available tabs.

Managing iSCSI Network

Special considerations apply to network adapters, both physical and VMkernel, that are associated with an iSCSI adapter.

After you create network connections for iSCSI, an iSCSI indicator becomes enabled in the vSphere Client. The indicator shows that a particular virtual or physical network adapter is iSCSI-bound. To avoid disruptions in iSCSI traffic, follow these guidelines and considerations when managing iSCSI-bound virtual and physical network adapters:

- Make sure that the VMkernel network adapters are assigned addresses on the same subnet as the iSCSI storage portal they connect to.
- iSCSI adapters using VMkernel adapters cannot connect to iSCSI ports on different subnets, even if the iSCSI adapters discover those ports.
- When using separate vSphere switches to connect physical network adapters and VMkernel adapters, make sure that the vSphere switches connect to different IP subnets.
- If VMkernel adapters are on the same subnet, they must connect to a single vSwitch.
- If you migrate VMkernel adapters to a different vSphere switch, move associated physical adapters.

- Do not make configuration changes to iSCSI-bound VMkernel adapters or physical network adapters.
- Do not make changes that might break association of VMkernel adapters and physical network adapters. You can break the association if you remove one of the adapters or the vSphere switch that connects them. Or if you change the 1:1 network policy for their connection.

iSCSI Network Troubleshooting

A warning sign indicates non-compliant port group policy for an iSCSI-bound VMkernel adapter.

The VMkernel adapter's port group policy is considered non-compliant in the following cases:

- The VMkernel adapter is not connected to an active physical network adapter.
- The VMkernel adapter is connected to more than one physical network adapter.
- The VMkernel adapter is connected to one or more standby physical adapters.
- The active physical adapter is changed.

Set up the correct network policy for the iSCSI-bound VMkernel adapter. See Setting Up Network for iSCSI and iSER.

Using Jumbo Frames with iSCSI and iSER

ESXi supports the use of Jumbo Frames with iSCSI/iSER.

Jumbo Frames are Ethernet frames with the size that exceeds 1500 Bytes. The maximum transmission unit (MTU) parameter is typically used to measure the size of Jumbo Frames.

When you use Jumbo Frames for iSCSI traffic, the following considerations apply:

- All network components must support Jumbo Frames.
- Check with your vendors to ensure your physical NICs and iSCSI adapters support Jumbo Frames.
- To set up and verify physical network switches for Jumbo Frames, consult your vendor documentation.

The following table explains the level of support that ESXi provides to Jumbo Frames.

Table 206: Support of Jumbo Frames

Type of iSCSI Adapters	Jumbo Frames Support
Software iSCSI	Supported
Dependent Hardware iSCSI	Supported. Check with vendor.
Independent Hardware iSCSI	Supported. Check with vendor.
VMware iSER	Supported. Check with vendor.

Enable Jumbo Frames for Networking

You can enable Jumbo Frames for ESXi storage adapters that use VMkernel networking for their traffic. These adapters include software iSCSI adapters, dependent hardware iSCSI adapters, and VMware iSER adapters.

To enable Jumbo Frames, change the default value of the maximum transmission units (MTU) parameter. You change the MTU parameter on the vSphere switch that you use for iSCSI traffic. For more information, see the *vSphere Networking* documentation.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Networking**, click **Virtual switches**, and select the vSphere switch that you want to modify from the list.
4. Click the **Edit settings** icon.
5. On the Properties page, change the MTU parameter.
   This step sets the MTU for all physical NICs on that standard switch. Set the MTU value to the largest MTU size among all NICs connected to the standard switch. ESXi supports the MTU size of up to 9000 Bytes.

Enable Jumbo Frames for Independent Hardware iSCSI

To enable Jumbo Frames for independent hardware iSCSI adapters on your ESXi host, change the default value of the maximum transmission units (MTU) parameter.

Use the Advanced Options settings to change the MTU parameter for the iSCSI HBA.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the independent hardware iSCSI adapter from the list of adapters.
4. Click the **Advanced Options** tab and click **Edit**.
5. Change the value of the MTU parameter.
   ESXi supports the MTU size up to 9000 Bytes.

Configure Dynamic or Static Discovery for iSCSI and iSER on ESXi Host

You need to set up target discovery addresses, so that the iSCSI or iSER storage adapter can determine which storage resource on the network is available for access.

Required privilege:**Host** > **Configuration** > **Storage Partition Configuration**

The ESXi system supports these discovery methods:

Dynamic Discovery	Also known as SendTargets discovery. Each time the initiator contacts a specified iSCSI server, the initiator sends the SendTargets request to the server. The server responds by supplying a list of available targets to the initiator. The names and IP addresses of these targets appear on the **Static Discovery** tab. If you remove a static target added by dynamic discovery, the target might be returned to the list the next time a rescan happens, the storage adapter is reset, or the host is rebooted. **Note:** With software and dependent hardware iSCSI, ESXi filters target addresses based on the IP family of the iSCSI server address specified. If the address is IPv4, IPv6 addresses that might come in the SendTargets response from the iSCSI server are filtered out. When DNS names are used to specify an iSCSI

	server, or when the SendTargets response from the iSCSI server has DNS names, ESXi relies on the IP family of the first resolved entry from DNS lookup.
Static Discovery	In addition to the dynamic discovery method, you can use static discovery and manually enter information for the targets. The iSCSI or iSER adapter uses a list of targets that you provide to contact and communicate with the iSCSI servers.

When you set up static or dynamic discovery, you can only add new iSCSI targets. You cannot change any parameters of an existing target. To make changes, remove the existing target and add a new one.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
4. Configure the discovery method.

Discovery Method	Description
Dynamic Discovery	1. Click **Dynamic Discovery** and click **Add**. 2. Enter the IP address or DNS name of the storage system and click **OK**. 3. Rescan the iSCSI adapter. After establishing the SendTargets session with the iSCSI system, your host populates the Static Discovery list with all newly discovered targets. **Note:** A dynamically discovered target remains on the list even after it is removed from the array side.
Static Discovery	1. Click **Static Discovery** and click **Add**. 2. Enter the target's information and click **OK** 3. Rescan the iSCSI adapter.

For other configuration steps you can perform for the iSCSI or iSER storage adapters, see the following topics:

- Set Up Independent Hardware iSCSI Adapters
- Configure Dependent Hardware iSCSI Adapters
- Configure the Software iSCSI Adapter
- Configure iSER with ESXi

Remove Dynamic or Static iSCSI Targets

Remove iSCSI servers connected to your ESXi host.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the iSCSI adapter to modify from the list.
4. Switch between **Dynamic Discovery** and **Static Discovery**.
5. Select an iSCSI server to remove and click **Remove**.
6. Rescan the iSCSI adapter.

   If you are removing the static target that was dynamically discovered, you need to remove it from the storage system before performing the rescan. Otherwise, your host will automatically discover and add the target to the list of static targets when you rescan the adapter.

Configuring CHAP Parameters for iSCSI or iSER Storage Adapters

Because the IP networks that the iSCSI technology uses to connect to remote targets do not protect the data they transport, you must ensure security of the connection. One of the protocols that iSCSI implements is the Challenge Handshake Authentication Protocol (CHAP), which verifies the legitimacy of initiators that access targets on the network.

CHAP uses a three-way handshake algorithm to verify the identity of your host and, if applicable, of the iSCSI target when the host and target establish a connection. The verification is based on a predefined private value, or CHAP secret, that the initiator and target share.

ESXi supports CHAP authentication at the adapter level. In this case, all targets receive the same CHAP name and secret from the iSCSI initiator. For software and dependent hardware iSCSI adapters, and for iSER adapters, ESXi also supports per-target CHAP authentication, which allows you to configure different credentials for each target to achieve greater level of security.

Selecting CHAP Authentication Method

ESXi supports unidirectional CHAP for all types of iSCSI/iSER initiators, and bidirectional CHAP for software and dependent hardware iSCSI, and for iSER.

Before configuring CHAP, check whether CHAP is enabled at the iSCSI storage system. Also, obtain information about the CHAP authentication method the system supports. If CHAP is enabled, configure it for your initiators, making sure that the CHAP authentication credentials match the credentials on the iSCSI storage.

ESXi supports the following CHAP authentication methods:

Unidirectional CHAP	In unidirectional CHAP authentication, the target authenticates the initiator, but the initiator does not authenticate the target.
Bidirectional CHAP	The bidirectional CHAP authentication adds an extra level of security. With this method, the initiator can also authenticate the target. VMware supports this method for software and dependent hardware iSCSI adapters, and for iSER adapters.

For software and dependent hardware iSCSI adapters, and for iSER adapters, you can set unidirectional CHAP and bidirectional CHAP for each adapter or at the target level. Independent hardware iSCSI supports CHAP only at the adapter level.

When you set the CHAP parameters, specify a security level for CHAP.

Note: When you specify the CHAP security level, how the storage array responds depends on the array's CHAP implementation and is vendor-specific. For information on CHAP authentication behavior in different initiator and target configurations, consult the array documentation.

Table 207: CHAP Security Level

CHAP Security Level	Description	Supported Storage Adapters
None	The host does not use CHAP authentication. If authentication is enabled, use this option to disable it.	Independent hardware iSCSI Software iSCSI Dependent hardware iSCSI iSER
Use unidirectional CHAP if required by target	The host prefers a non-CHAP connection, but can use a CHAP connection if required by the target.	Software iSCSI Dependent hardware iSCSI iSER
Use unidirectional CHAP unless prohibited by target	The host prefers CHAP, but can use non-CHAP connections if the target does not support CHAP.	Independent hardware iSCSI Software iSCSI

CHAP Security Level	Description	Supported Storage Adapters
		Dependent hardware iSCSI iSER
Use unidirectional CHAP	The host requires successful CHAP authentication. The connection fails if CHAP negotiation fails.	Independent hardware iSCSI Software iSCSI Dependent hardware iSCSI iSER
Use bidirectional CHAP	The host and the target support bidirectional CHAP.	Software iSCSI Dependent hardware iSCSI iSER

Set Up CHAP for iSCSI or iSER Storage Adapter

When you set up CHAP name and secret at the iSCSI/iSER adapter level, all targets receive the same parameters from the adapter. By default, all discovery addresses or static targets inherit CHAP parameters that you set up at the adapter level.

- Before setting up CHAP parameters for software or dependent hardware iSCSI, determine whether to configure unidirectional or bidirectional CHAP. Independent hardware iSCSI adapters do not support bidirectional CHAP.
- Verify CHAP parameters configured on the storage side. Parameters that you configure must match the ones on the storage side.
- Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

The CHAP name cannot exceed 511 alphanumeric characters and the CHAP secret cannot exceed 255 alphanumeric characters. Some adapters, for example the QLogic adapter, might have lower limits, 255 for the CHAP name and 100 for the CHAP secret.

1. Navigate to the iSCSI or iSER storage adapter.
   a) In the vSphere Client, navigate to the ESXi host.
   b) Click the **Configure** tab.
   c) Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
2. Click the **Properties** tab and click **Edit** in the **Authentication** panel.
3. Specify authentication method.
   - **None**
   - **Use unidirectional CHAP if required by target**
   - **Use unidirectional CHAP unless prohibited by target**
   - **Use unidirectional CHAP**
   - **Use bidirectional CHAP**. To configure bidirectional CHAP, you must select this option.
4. Specify the outgoing CHAP name.

   Make sure that the name you specify matches the name configured on the storage side.
   - To set the CHAP name to the iSCSI adapter name, select **Use initiator name**.
   - To set the CHAP name to anything other than the iSCSI initiator name, deselect **Use initiator name** and enter a name in the **Name** text box.
5. Enter an outgoing CHAP secret to be used as part of authentication. Use the same secret that you enter on the storage side.
6. If configuring bidirectional CHAP, specify incoming CHAP credentials.

   Make sure to use different secrets for the outgoing and incoming CHAP.

7. Click **OK**.
8. Rescan the iSCSI adapter.

If you change the CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and log in again.

For other configuration steps you can perform for the iSCSI or iSER storage adapters, see the following topics:
- Set Up Independent Hardware iSCSI Adapters
- Configure Dependent Hardware iSCSI Adapters
- Configure the Software iSCSI Adapter
- Configure iSER with ESXi

Set Up CHAP for Target

If you use software and dependent hardware iSCSI adapters, or an iSER storage adapter, you can configure different CHAP credentials for each discovery address or static target.

- Before setting up CHAP parameters, determine whether to configure unidirectional or bidirectional CHAP.
- Verify CHAP parameters configured on the storage side. Parameters that you configure must match the ones on the storage side.
- Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

The CHAP name cannot exceed 511 and the CHAP secret 255 alphanumeric characters.

1. Navigate to the iSCSI or iSER storage adapter.
   a) In the vSphere Client, navigate to the ESXi host.
   b) Click the **Configure** tab.
   c) Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
2. Click either **Dynamic Discovery** or **Static Discovery**.
3. From the list of available targets, select a target to configure and click **Authentication**.
4. Deselect **Inherit settings from parent** and specify authentication method.
   - **None**
   - **Use unidirectional CHAP if required by target**
   - **Use unidirectional CHAP unless prohibited by target**
   - **Use unidirectional CHAP**
   - **Use bidirectional CHAP**. To configure bidirectional CHAP, you must select this option.
5. Specify the outgoing CHAP name.

   Make sure that the name you specify matches the name configured on the storage side.
   - To set the CHAP name to the iSCSI adapter name, select **Use initiator name**.
   - To set the CHAP name to anything other than the iSCSI initiator name, deselect **Use initiator name** and enter a name in the **Name** text box.
6. Enter an outgoing CHAP secret to be used as part of authentication. Use the same secret that you enter on the storage side.
7. If configuring bidirectional CHAP, specify incoming CHAP credentials.

   Make sure to use different secrets for the outgoing and incoming CHAP.

8. Click **OK**.
9. Rescan the storage adapter.

If you change the CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and login again.

Configuring Advanced Parameters for iSCSI

You might need to configure additional parameters for iSCSI initiators on your ESXi host. For example, some iSCSI storage systems require ARP (Address Resolution Protocol) redirection to move iSCSI traffic dynamically from one port to another. In this case, you must activate the ARP redirection on your host.

The following table lists advanced iSCSI parameters that you can configure using the vSphere Client. In addition, you can use the vSphere CLI commands to configure some of the advanced parameters. For information, see the *Getting Started with ESXCLI* documentation.

Depending on the type of your adapters, certain parameters might not be available.

Important: Do not change the advanced iSCSI settings unless VMware support or Storage Vendors direct you to change them.

Table 208: Additional Parameters for iSCSI Initiators

Advanced Parameter	Description
Header Digest	Increases data integrity. When the header digest parameter is enabled, the system performs a checksum over each header part of the iSCSI Protocol Data Unit (PDU). The system verifies the data using the CRC32C algorithm.
Data Digest	Increases data integrity. When the data digest parameter is enabled, the system performs a checksum over each PDU data part. The system verifies the data using the CRC32C algorithm. **Note:** Systems that use the Intel Nehalem processors offload the iSCSI digest calculations for software iSCSI. This offload helps to reduce the impact on performance.
ErrorRecoveryLevel	iSCSI Error Recovery Level (ERL) value that the iSCSI initiator on the host negotiates during a login.
LoginRetryMax	Maximum number of times the ESXi iSCSI initiator attempts to log into a target before ending the attempts.
MaxOutstandingR2T	Defines the R2T (Ready to Transfer) PDUs that can be in transition before an acknowledge PDU is received.
FirstBurstLength	Specifies the maximum amount of unsolicited data an iSCSI initiator can send to the target during the execution of a single SCSI command, in bytes.
MaxBurstLength	Maximum SCSI data payload in a Data-In or a solicited Data-Out iSCSI sequence, in bytes.
MaxRecvDataSegLength	Maximum data segment length, in bytes, that can be received in an iSCSI PDU.
MaxCommands	Maximum SCSI commands that can be queued on the iSCSI adapter.
DefaultTimeToWait	Minimum time in seconds to wait before attempting a logout or an active task reassignment after an unexpected connection termination or reset.
DefautTimeToRetain	Maximum time in seconds, during which reassigning the active task is still possible after a connection termination or reset.
LoginTimeout	Time in seconds the initiator will wait for the login response to finish.
LogoutTimeout	Time in seconds initiator will wait to get a response for Logout request PDU.
RecoveryTimeout	Specifies the amount of time, in seconds, that can lapse while a session recovery is performed. If the timeout exceeds its limit, the iSCSI initiator ends the session.

Advanced Parameter	Description
No-Op Interval	Specifies the time interval, in seconds, between NOP-Out requests sent from your iSCSI initiator to an iSCSI target. The NOP-Out requests serve as the ping mechanism to verify that a connection between the iSCSI initiator and the iSCSI target is active.
No-Op Timeout	Specifies the amount of time, in seconds, that can lapse before your host receives a NOP-In message. The iSCSI target sends the message in response to the NOP-Out request. When the no-op timeout limit is exceeded, the initiator ends the current session and starts a new one.
ARP Redirect	With this parameter enabled, storage systems can move iSCSI traffic dynamically from one port to another. Storage systems that perform array-based failovers require the ARP parameter.
Delayed ACK	With this parameter enabled, storage systems can delay an acknowledgment of received data packets.

Configure Advanced Parameters for iSCSI on ESXi Host

The advanced iSCSI settings control such parameters as header and data digest, ARP redirection, delayed ACK, and so on.

Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

CAUTION: Do not make any changes to the advanced iSCSI settings unless you are working with the VMware support team or otherwise have thorough information about the values to provide for the settings.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
4. Configure advanced parameters.

Option	Description
At the adapter level	Click the **Advanced Options** tab and click **Edit**.
At the target level	1. Click either **Dynamic Discovery** or **Static Discovery**. 2. From the list of available targets, select a target to configure and click **Advanced**.

5. Enter any required values for the advanced parameters you want to modify.

iSCSI Session Management

To communicate with each other, iSCSI initiators and targets establish iSCSI sessions. You can review and manage iSCSI sessions using vSphere CLI.

By default, software iSCSI and dependent hardware iSCSI initiators start one iSCSI session between each initiator port and each target port. If your iSCSI initiator or target has more than one port, your host can have multiple sessions established. The default number of sessions for each target equals the number of ports on the iSCSI adapter times the number of target ports.

Using vSphere CLI, you can display all current sessions to analyze and debug them. To create more paths to storage systems, you can increase the default number of sessions by duplicating existing sessions between the iSCSI adapter and target ports.

You can also establish a session to a specific target port. This capability is useful if your host connects to a single-port storage system that presents only one target port to your initiator. The system then redirects additional sessions to a different target port. Establishing a new session between your iSCSI initiator and another target port creates an additional path to the storage system.

The following considerations apply to iSCSI session management:

- Some storage systems do not support multiple sessions from the same initiator name or endpoint. Attempts to create multiple sessions to such targets can result in an unpredictable behavior of your iSCSI environment.
- Storage vendors can provide automatic session managers. Using the automatic session manages to add or delete sessions, does not guarantee lasting results and can interfere with the storage performance.

Review iSCSI Sessions

Use the vCLI command to display iSCSI sessions between an iSCSI adapter and a storage system.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To list iSCSI sessions, run the following command:

```
esxcli iscsi session list
```

The command takes these options:

Option	Description
-A|--adapter=*str*	The iSCSI adapter name, for example, vmhba34.
-s|--isid=*str*	The iSCSI session identifier.
-n|--name=*str*	The iSCSI target name, for example, iqn.X.

Add iSCSI Sessions

Use the vCLI to add an iSCSI session for a target you specify or to duplicate an existing session. By duplicating sessions, you increase the default number of sessions and create additional paths to storage systems.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To add or duplicate an iSCSI session, run the following command:

```
esxcli iscsi session add
```

The command takes these options:

Option	Description
-A|--adapter=*str*	The iSCSI adapter name, for example, vmhba34. This option is required.
-s|--isid=*str*	The ISID of a session to duplicate. You can find it by listing all sessions.
-n|--name=*str*	The iSCSI target name, for example, iqn.X.

Rescan the iSCSI adapter.

Remove iSCSI Sessions

Use the vCLI command to remove an iSCSI session between an iSCSI adapter and a target.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To remove a session, run the following command:

```
esxcli iscsi session remove
```

The command takes these options:

Option	Description
-A|--adapter=*str*	The iSCSI adapter name, for example, vmhba34. This option is required.
-s|--isid=*str*	The ISID of a session to remove. You can find it by listing all session.

Option	Description
-n|--name=*str*	The iSCSI target name, for example, iqn.X.

Rescan the iSCSI adapter.

Booting from iSCSI SAN with ESXi

When you set up your ESXi host to boot from a SAN, your host's boot image is stored on one or more LUNs in the SAN storage system. When the ESXi host starts, it boots from the LUN on the SAN rather than from its local disk.

You can use boot from the SAN if you do not want to handle maintenance of local storage or have diskless hardware configurations, such as blade systems.

ESXi supports different methods of booting from the iSCSI SAN.

Table 209: Boot from iSCSI SAN support

Independent Hardware iSCSI	Software iSCSI
Configure the iSCSI HBA to boot from the SAN. For information on configuring the HBA, see Configure Independent Hardware iSCSI Adapter for SAN Boot.	Use the software iSCSI adapter and a network adapter that supports the iSCSI Boot Firmware Table (iBFT) format. For information, see *VMware ESXi Installation and Setup*.

General Recommendations for Boot from iSCSI SAN

If you plan to set up and use an iSCSI LUN as the boot device for your host, follow certain general guidelines.

The following guidelines apply to booting from the independent hardware iSCSI and iBFT.

- Review any vendor recommendations for the hardware you use in your boot configuration.
- For installation prerequisites and requirements, review *vSphere Installation and Setup*.
- Use static IP addresses to reduce the chances of DHCP conflicts.
- Use different LUNs for VMFS datastores and boot partitions.
- Configure proper ACLs on your storage system.
  - The boot LUN must be visible only to the host that uses the LUN. No other host on the SAN is permitted to see that boot LUN.
  - If a LUN is used for a VMFS datastore, multiple hosts can share the LUN.
- Configure a diagnostic partition.
  - With the independent hardware iSCSI only, you can place the diagnostic partition on the boot LUN. If you configure the diagnostic partition in the boot LUN, this LUN cannot be shared across multiple hosts. If a separate LUN is used for the diagnostic partition, multiple hosts can share the LUN.
  - If you boot from SAN using iBFT, you cannot set up a diagnostic partition on a SAN LUN. To collect your host's diagnostic information, use the vSphere ESXi Dump Collector on a remote server. For information about the ESXi Dump Collector, see *vCenter Server Installation and Setup* and *vSphere Networking*.

Prepare the iSCSI SAN

Before you configure your host to boot from an iSCSI LUN, prepare and configure your storage area network.

CAUTION: If you use scripted installation to install ESXi when booting from a SAN, you must take special steps to avoid unintended data loss.

1. Connect network cables, referring to any cabling guide that applies to your setup.
2. Ensure IP connectivity between your storage system and server.

   Verify configuration of any routers or switches on your storage network. Storage systems must be able to ping the iSCSI adapters in your hosts.
3. Configure the storage system.
   a) Create a volume (or LUN) on the storage system for your host to boot from.
   b) Configure the storage system so that your host has access to the assigned LUN.

      This step might involve updating ACLs with the IP addresses, iSCSI names, and the CHAP authentication parameter you use on your host. On some storage systems, in addition to providing access information for the ESXi host, you must also explicitly associate the assigned LUN with the host.
   c) Ensure that the LUN is presented to the host correctly.
   d) Ensure that no other system has access to the configured LUN.
   e) Record the iSCSI name and IP addresses of the targets assigned to the host.

      You must have this information to configure your iSCSI adapters.

Configure Independent Hardware iSCSI Adapter for SAN Boot

If your ESXi host uses an independent hardware iSCSI adapter, such as QLogic HBA, you can configure the adapter to boot from the SAN.

This procedure discusses how to enable the QLogic iSCSI HBA to boot from the SAN. For more information and more up-to-date details about QLogic adapter configuration settings, see the QLogic website.

1. Start the installation media and reboot the host.
2. Use the BIOS to set the host to boot from the installation media first.
3. During server POST, press Crtl+q to enter the QLogic iSCSI HBA configuration menu.
4. Select the I/O port to configure.

   By default, the Adapter Boot mode is set to Disable.
5. Configure the HBA.
   a) From the **Fast!UTIL Options** menu, select **Configuration Settings** > **Host Adapter Settings**.
   b) Optional: Configure the following settings for your host adapter: initiator IP address, subnet mask, gateway, initiator iSCSI name, and CHAP.
6. Configure iSCSI settings.

   See Configure iSCSI Boot Settings.

7. Save your changes and restart the system.

Configure iSCSI Boot Settings

Configure iSCSI boot parameters, so that your ESXi host can boot from an iSCSI LUN.

1. From the **Fast!UTIL Options** menu, select **Configuration Settings** > **iSCSI Boot Settings**.
2. Before you can set SendTargets, set Adapter Boot mode to **Manual**.
3. Select **Primary Boot Device Settings**.
   a) Enter the discovery **Target IP** and **Target Port**.
   b) Configure the **Boot LUN** and **iSCSI Name** parameters.
      - If only one iSCSI target and one LUN are available at the target address, leave **Boot LUN** and **iSCSI Name** blank.
        After your host reaches the target storage system, these text boxes are populated with appropriate information.
      - If more than one iSCSI target and LUN are available, supply values for **Boot LUN** and **iSCSI Name**.
   c) Save changes.
4. From the **iSCSI Boot Settings** menu, select the primary boot device.
   An auto rescan of the HBA finds new target LUNs.
5. Select the iSCSI target.
   If more than one LUN exists within the target, you can select a specific LUN ID by pressing **Enter** after you locate the iSCSI device.
6. Return to the **Primary Boot Device Setting** menu. After the rescan, **Boot LUN** and **iSCSI Name** are populated. Change the value of **Boot LUN** to the appropriate LUN ID.

Best Practices for iSCSI Storage

When using ESXi with the iSCSI SAN, follow recommendations that VMware offers to avoid problems.

Check with your storage representative if your storage system supports Storage API - Array Integration hardware acceleration features. If it does, refer to your vendor documentation to enable hardware acceleration support on the storage system side. For more information, see Storage Hardware Acceleration.

Preventing iSCSI SAN Problems

When using ESXi with a SAN, you must follow specific guidelines to avoid SAN problems.

Observe the following tips:

- Place only one VMFS datastore on each LUN.
- Do not change the path policy the system sets for you unless you understand the implications of making such a change.
- Document everything. Include information about configuration, access control, storage, switch, server and iSCSI HBA configuration, software and firmware versions, and storage cable plan.
- Plan for failure:
  – Make several copies of your topology maps. For each element, consider what happens to your SAN if the element fails.
  – Cross off different links, switches, HBAs, and other elements to ensure that you did not miss a critical failure point in your design.
- Ensure that the iSCSI HBAs are installed in the correct slots in the ESXi host, based on slot and bus speed. Balance PCI bus load among the available buses in the server.

- Become familiar with the various monitor points in your storage network, at all visibility points, including ESXi performance charts, Ethernet switch statistics, and storage performance statistics.
- Change LUN IDs only when VMFS datastores deployed on the LUNs have no running virtual machines. If you change the ID, virtual machines running on the VMFS datastore might fail.

  After you change the ID of the LUN, you must rescan your storage to reset the ID on your host. For information on using the rescan, see Storage Rescan Operations.
- If you change the default iSCSI name of your iSCSI adapter, make sure that the name you enter is worldwide unique and properly formatted. To avoid storage access problems, never assign the same iSCSI name to different adapters, even on different hosts.

Optimizing iSCSI SAN Storage Performance

Several factors contribute to optimizing a typical SAN environment.

If the network environment is properly configured, the iSCSI components provide adequate throughput and low enough latency for iSCSI initiators and targets. If the network is congested and links, switches or routers are saturated, iSCSI performance suffers and might not be adequate for ESXi environments.

Storage System Performance

Storage system performance is one of the major factors contributing to the performance of the entire iSCSI environment.

If issues occur with storage system performance, consult your storage system vendor’s documentation for any relevant information.

When you assign LUNs, remember that you can access each shared LUN through a number of hosts, and that a number of virtual machines can run on each host. One LUN used by the ESXi host can service I/O from many different applications running on different operating systems. Because of this diverse workload, the RAID group that contains the ESXi LUNs should not include LUNs that other hosts use that are not running ESXi for I/O intensive applications.

Enable read caching and write caching.

Load balancing is the process of spreading server I/O requests across all available SPs and their associated host server paths. The goal is to optimize performance in terms of throughput (I/O per second, megabytes per second, or response times).

SAN storage systems require continual redesign and tuning to ensure that I/O is load balanced across all storage system paths. To meet this requirement, distribute the paths to the LUNs among all the SPs to provide optimal load balancing. Close monitoring indicates when it is necessary to manually rebalance the LUN distribution.

Tuning statically balanced storage systems is a matter of monitoring the specific performance statistics (such as I/O operations per second, blocks per second, and response time) and distributing the LUN workload to spread the workload across all the SPs.

Server Performance with iSCSI

To ensure optimal ESXi host performance, consider several factors.

Each server application must have access to its designated storage with the following conditions:

- High I/O rate (number of I/O operations per second)
- High throughput (megabytes per second)
- Minimal latency (response times)

Because each application has different requirements, you can meet these goals by selecting an appropriate RAID group on the storage system.

To achieve performance goals, follow these guidelines:

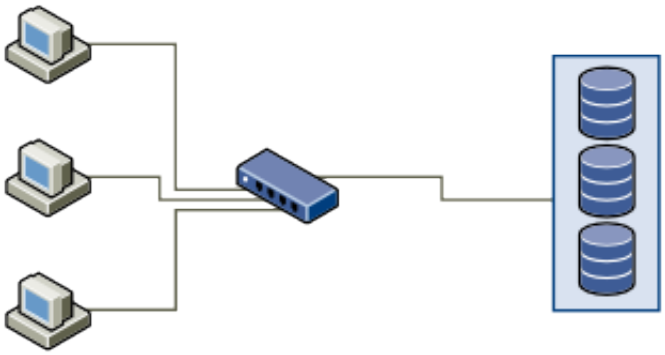
- Place each LUN on a RAID group that provides the necessary performance levels. Monitor the activities and resource use of other LUNS in the assigned RAID group. A high-performance RAID group that has too many applications doing I/O to it might not meet performance goals required by an application running on the ESXi host.
- To achieve maximum throughput for all the applications on the host during the peak period, install enough network adapters or iSCSI hardware adapters. I/O spread across multiple ports provides faster throughput and less latency for each application.
- To provide redundancy for software iSCSI, make sure that the initiator is connected to all network adapters used for iSCSI connectivity.
- When allocating LUNs or RAID groups for ESXi systems, remember that multiple operating systems use and share that resource. The LUN performance required by the ESXi host might be much higher than when you use regular physical machines. For example, if you expect to run four I/O intensive applications, allocate four times the performance capacity for the ESXi LUNs.
- When you use multiple ESXi systems with vCenter Server, the storage performance requirements increase.
- The number of outstanding I/Os needed by applications running on an ESXi system must match the number of I/Os the SAN can handle.

Network Performance

A typical SAN consists of a collection of computers connected to a collection of storage systems through a network of switches. Several computers often access the same storage.

The following graphic shows several computer systems connected to a storage system through an Ethernet switch. In this configuration, each system is connected through a single Ethernet link to the switch. The switch is connected to the storage system through a single Ethernet link.

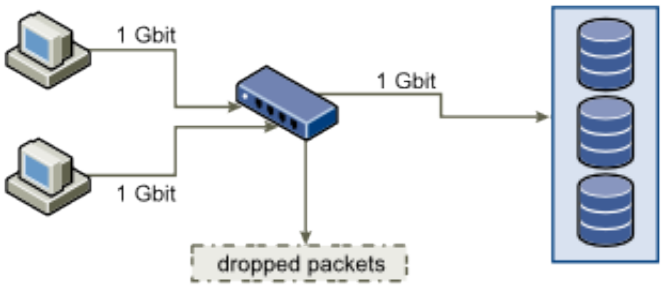
Figure 70: Single Ethernet Link Connection to Storage



When systems read data from storage, the storage responds with sending enough data to fill the link between the storage systems and the Ethernet switch. It is unlikely that any single system or virtual machine gets full use of the network speed. However, this situation can be expected when many systems share one storage device.

When writing data to storage, multiple systems or virtual machines might attempt to fill their links. As a result, the switch between the systems and the storage system might drop network packets. The data drop might occur because the switch has more traffic to send to the storage system than a single link can carry. The amount of data the switch can transmit is limited by the speed of the link between it and the storage system.

Figure 71: Dropped Packets



Recovering from dropped network packets results in large performance degradation. In addition to time spent determining that data was dropped, the retransmission uses network bandwidth that can otherwise be used for current transactions.

iSCSI traffic is carried on the network by the Transmission Control Protocol (TCP). TCP is a reliable transmission protocol that ensures that dropped packets are retried and eventually reach their destination. TCP is designed to recover from dropped packets and retransmits them quickly and seamlessly. However, when the switch discards packets with any regularity, network throughput suffers. The network becomes congested with requests to resend data and with the resent packets. Less data is transferred than in a network without congestion.

Most Ethernet switches can buffer, or store, data. This technique gives every device attempting to send data an equal chance to get to the destination. The ability to buffer some transmissions, combined with many systems limiting the number of outstanding commands, reduces transmissions to small bursts. The bursts from several systems can be sent to a storage system in turn.

If the transactions are large and multiple servers are sending data through a single switch port, an ability to buffer can be exceeded. In this case, the switch drops the data it cannot send, and the storage system must request a retransmission of the dropped packet. For example, if an Ethernet switch can buffer 32 KB, but the server sends 256 KB to the storage device, some of the data is dropped.

Most managed switches provide information on dropped packets, similar to the following:

```
*: interface is up
IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count
```

Table 210: Sample Switch Information

Interface	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

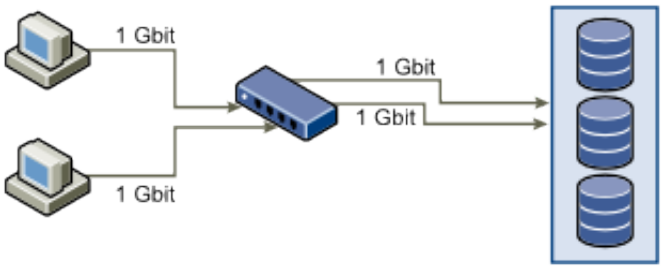
In this example from a Cisco switch, the bandwidth used is 476303000 bits/second, which is less than half of wire speed. The port is buffering incoming packets, but has dropped several packets. The final line of this interface summary indicates that this port has already dropped almost 10,000 inbound packets in the IQD column.

Configuration changes to avoid this problem involve making sure several input Ethernet links are not funneled into one output link, resulting in an oversubscribed link. When several links transmitting near capacity are switched to a smaller number of links, oversubscription becomes possible.

Generally, applications or systems that write much data to storage must avoid sharing Ethernet links to a storage device. These types of applications perform best with multiple connections to storage devices.

Multiple Connections from Switch to Storage shows multiple connections from the switch to the storage.

Figure 72: Multiple Connections from Switch to Storage



Using VLANs or VPNs does not provide a suitable solution to the problem of link oversubscription in shared configurations. VLANs and other virtual partitioning of a network provide a way of logically designing a network. However, they do not change the physical capabilities of links and trunks between switches. When storage traffic and other network traffic share physical connections, oversubscription and lost packets might become possible. The same is true of VLANs that share interswitch trunks. Performance design for a SAN must consider the physical limitations of the network, not logical allocations.

Checking Ethernet Switch Statistics

Many Ethernet switches provide different methods for monitoring switch health.

Switches that have ports operating near maximum throughput much of the time do not provide optimum performance. If you have ports in your iSCSI SAN running near the maximum, reduce the load. If the port is connected to an ESXi system or iSCSI storage, you can reduce the load by using manual load balancing.

If the port is connected between multiple switches or routers, consider installing additional links between these components to handle more load. Ethernet switches also commonly provide information about transmission errors, queued packets, and dropped Ethernet packets. If the switch regularly reports any of these conditions on ports being used for iSCSI traffic, performance of the iSCSI SAN will be poor.

Managing Storage Devices

Manage local and networked storage device that your ESXi host has access to.

Storage Device Characteristics

When your ESXi host connects to block-based storage systems, LUNs or storage devices that support ESXi become available to the host.

After the devices get registered with your host, you can display all available local and networked devices and review their information. If you use third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

Note: If an array supports implicit asymmetric logical unit access (ALUA) and has only standby paths, the registration of the device fails. The device can register with the host after the target activates a standby path and the host detects it as active. The advanced system `/Disk/FailDiskRegistration` parameter controls this behavior of the host.

For each storage adapter, you can display a separate list of storage devices available for this adapter.

Generally, when you review storage devices, you see the following information.

Table 211: Storage Device Information

Storage Device Information	Description
Name	Also called Display Name. It is a name that the ESXi host assigns to the device based on the storage type and manufacturer. Generally, you can change this name to a name of your choice. See Rename Storage Devices.
Identifier	A universally unique identifier that is intrinsic to the device. See Storage Device Names and Identifiers.
Operational State	Indicates whether the device is attached or detached. See Detach Storage Devices.
LUN	Logical Unit Number (LUN) within the SCSI target. The LUN number is provided by the storage system. If a target has only one LUN, the LUN number is always zero (0).
Type	Type of device, for example, disk or CD-ROM.
Drive Type	Information about whether the device is a flash drive or a regular HDD drive. For information about flash drives and NVMe devices, see Working with Flash Devices.
Transport	Transportation protocol your host uses to access the device. The protocol depends on the type of storage being used. See Types of Physical Storage.
Capacity	Total capacity of the storage device.
Owner	The plug-in, such as the NMP or a third-party plug-in, that the host uses to manage paths to the storage device. See Pluggable Storage Architecture and Path Management.
Hardware Acceleration	Information about whether the storage device assists the host with virtual machine management operations. The status can be Supported, Not Supported, or Unknown. See Storage Hardware Acceleration.
Sector Format	Indicates whether the device uses a traditional, 512n, or advanced sector format, such as 512e or 4Kn. See Device Sector Formats.
Location	A path to the storage device in the `/vmfs/devices/` directory.
Partition Format	A partition scheme used by the storage device. It can be of a master boot record (MBR) or GUID partition table (GPT) format. The GPT devices can support datastores greater than 2 TB. See Device Sector Formats.
Partitions	Primary and logical partitions, including a VMFS datastore, if configured.
Multipathing Policies	Path Selection Policy and Storage Array Type Policy the host uses to manage paths to storage. See Understanding Multipathing and Failover.
Paths	Paths used to access storage and their status. See Disable Storage Paths.

Display Storage Devices for an ESXi Host

Display all storage devices available to a ESXi host. If you use any third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

The Storage Devices view allows you to list the hosts' storage devices, analyze their information, and modify properties.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
   All storage devices available to the host are listed in the Storage Devices table.

4. To view details for a specific device, select the device from the list.
5. Use the icons to perform basic storage management tasks.

   Availability of specific icons depends on the device type and configuration.

Icon	Description
Refresh	Refresh information about storage adapters, topology, and file systems.
Detach	Detach the selected device from the host.
Attach	Attach the selected device to the host.
Rename	Change the display name of the selected device.
Turn On LED	Turn on the locator LED for the selected devices.
Turn Off LED	Turn off the locator LED for the selected devices.
Mark as Flash Disk	Mark the selected devices as flash disks.
Mark as HDD Disk	Mark the selected devices as HDD disks.
Mark as Local	Mark the selected devices as local for the host.
Mark as Remote	Mark the selected devices as remote for the host.
Erase Partitions	Erase partitions on the selected devices.
Mark as Perennially Reserved	Mark the selected device as perennially reserved.
Unmark as Perennially Reserved	Clear the perennial reservation from the selected device.

6. Use the following tabs to access additional information and modify properties for the selected device.

Tab	Description
Properties	View device properties and characteristics. View and modify multipathing policies for the device.
Paths	Display paths available for the device. Disable or enable a selected path.
Partition Details	Displays information about partitions and their formats.

Display Storage Devices for an Adapter

Display a list of storage devices accessible through a specific storage adapter on an ESXi host.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**.

   All storage adapters installed on the host are listed in the Storage Adapters table.
4. Select the adapter from the list and click the **Devices** tab.

   Storage devices that the host can access through the adapter are displayed.

5. Use the icons to perform basic storage management tasks.

   Availability of specific icons depends on the device type and configuration.

Icon	Description
Refresh	Refresh information about storage adapters, topology, and file systems.
Detach	Detach the selected device from the host.
Attach	Attach the selected device to the host.
Rename	Change the display name of the selected device.

Device Sector Formats

ESXi supports storage devices with traditional and advanced sector formats. In storage, a sector is a subdivision of a track on a storage disk or device. Each sector stores a fixed amount of data.

This table introduces different storage device formats that ESXi supports.

Storage Device Format	ESXi Software Emulation	Logical Sector Size	Physical Sector Size	VMFS Datastore
512n	N/A	512	512	VMFS5 and VMFS6 (default)
512e	N/A	512	4096	VMFS5 and VMFS56 (default) **Note:** Local 512e storage devices do not support VMFS5.
4Kn	512	4096	4096	VMFS6

512-Byte Native Format

ESXi supports traditional 512n storage devices that use a native 512-bytes sector size.

512-Byte Emulation Format

Due to the increasing demand for larger capacities, the storage industry has introduced advanced formats, such as 512-byte emulation, or 512e. 512e is the advanced format in which the physical sector size is 4096 bytes, but the logical sector emulates 512-bytes sector size. Storage devices that use the 512e format can support legacy applications and guest operating systems. These devices serve as an intermediate step to 4Kn sector drives.

4K Native Format with Software Emulation

Another advanced format that ESXi supports is the 4Kn sector technology. In the 4Kn devices, both physical and logical sectors are 4096 bytes (4 KiB) in length. The device does not have an emulation layer, but exposes its 4Kn physical sector size directly to ESXi.

ESXi detects and registers the 4Kn devices and automatically emulates them as 512e. The device is presented to upper layers in ESXi as 512e. But the guest operating systems always see it as a 512n device. You can continue using existing VMs with legacy guest OSes and applications on the host with the 4Kn devices.

When you use 4Kn devices, the following considerations apply:

- ESXi supports only local 4Kn SAS and SATA HDDs.

- ESXi does not support 4Kn SSD and NVMe devices, or 4Kn devices as RDMs.
- ESXi can boot only from a 4Kn device with UEFI.
- You can use the 4Kn device to configure a coredump partition and coredump file.
- Only the NMP plug-in can claim the 4Kn devices. You cannot use the HPP to claim these devices.
- With vSAN, you can use only the 4Kn capacity HDDs for vSAN Hybrid Arrays. For information, see the *Administering VMware vSAN* documentation.
- Due to the software emulation layer, the performance of the 4Kn devices depends on the alignment of the I/Os. For best performance, run workloads that issue mostly 4K aligned I/Os.
- Workloads accessing the emulated 4Kn device directly using scatter-gather I/O (SGIO) must issue I/Os compatible with the 512e disk.

Determine Device Format

To determine whether the device uses the 512n, 512e, or 4Kn format, run the following command.

```
esxcli storage core device capacity list
```

The following sample output shows the format type.

```
Device                Physical Blocksize  Logical Blocksize  Logical Block Count         Size  For-
mat Type
--------------------  ------------------  -----------------  -------------------  -----------
 -----------
naa.5000xxxxxxxxx36f                 512                512           2344225968  1144641 MiB  512n
naa.5000xxxxxxxxx030                4096                512           3516328368  1716957 MiB  4Kn
 SWE
naa.5000xxxxxxxxx8df                 512                512           2344225968  1144641 MiB  512n
naa.5000xxxxxxxxx4f4                4096                512           3516328368  1716957 MiB  4Kn
 SWE
```

Storage Device Names and Identifiers

In the ESXi environment, each storage device is identified by several names.

Device Identifiers

Depending on the type of storage, the ESXi host uses different algorithms and conventions to generate an identifier for each storage device.

Storage-provided identifiers

The ESXi host queries a target storage device for the device name. From the returned metadata, the host extracts or generates a unique identifier for the device. The identifier is based on specific storage standards, is unique and persistent across all hosts, and has one of the following formats:

- naa.*xxx*
- eui.*xxx*
- t10.*xxx*

Path-based identifier

When the device does not provide an identifier, the host generates an mpx.*path* name, where *path* represents the first path to the device, for example, `mpx.vmhba1:C0:T1:L3`. This identifier can be used in the same way as the storage-provided identifies.

The mpx.*path* identifier is created for local devices on the assumption that their path names are unique. However, this

identifier is not unique or persistent, and can change after every system restart.

Typically, the path to the device has the following format:

vmhba*Adapter*:C*Channel*:T*Target*:L*LUN*

- vmhba*Adapter* is the name of the storage adapter. The name refers to the physical adapter on the host, not to the SCSI controller used by the virtual machines.
- C*Channel* is the storage channel number.
  Software iSCSI adapters and dependent hardware adapters use the channel number to show multiple paths to the same target.
- T*Target* is the target number. Target numbering is determined by the host and might change when the mappings of targets visible to the host change. Targets that are shared by different hosts might not have the same target number.
- L*LUN* is the LUN number that shows the position of the LUN within the target. The LUN number is provided by the storage system. If a target has only one LUN, the LUN number is always zero (0).

For example, `vmhba1:C0:T3:L1` represents LUN1 on target 3 accessed through the storage adapter vmhba1 and channel 0.

Legacy identifier

In addition to the device-provided identifiers or mpx.*path* identifiers, ESXi generates an alternative legacy name for each device. The identifier has the following format:

vml.*number*

The legacy identifier includes a series of digits that are unique to the device. The identifier can be derived in part from the metadata obtained through the SCSI INQUIRY command. For nonlocal devices that do not provide SCSI INQUIRY identifiers, the vml.*number* identifier is used as the only available unique identifier.

Displaying Device Names in the vSphere CLI

You can use the `esxcli storage core device list` command to display all device names in the vSphere CLI. The output is similar to the following example:

```
# esxcli storage core device list
naa.XXX
   Display Name: DGC Fibre Channel Disk(naa.XXX)
   ...
   Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
   Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
   ...
   Other UIDs: vml.0000000000XYZ
```

NVMe Devices with NGUID Device Identifiers

For NVMe devices, ESXi generates device identifiers based on the information it retrieves from the devices. Generally, the NVMe devices support identifiers in EUI64 or NGUID formats, or use both formats. NGUID is a Namespace Globally Unique Identifier that uses the EUI64 16-byte designator format.

For the devices that support only NGUID format, the host-generated device identifier changes depending on the version of ESXi. The ESXi host of version 6.7 and earlier created the t10.*xxx_controller_serial_number* identifier. Starting with 6.7 Update 1, the host creates two identifiers: eui.*xxx (NGUID)* as primary and t10.*xxx_controller_serial_number* as alternative primary.

ID Formats Supported by Device		Device Identifier Generated by Host	
EUI64 ID Format	**NGUID ID Format**	**ESXi 6.7 and earlier**	**ESXi 6.7 Update 1 and later**
yes	yes	t10.*xxx_EUI64*	t10.*xxx_EUI64*
yes	no	t10.*xxx_EUI64*	t10.*xxx_EUI64*
no	yes	t10.*xxx_controller_serial_number*	eui.*xxx (NGUID)* as primary ID t10.*xxx_controller_serial_number* as alternative primary ID

Note: If your host has NGUID-only devices and you upgrade the host to ESXi 7.0.x from an earlier version, the device identifier changes from t10.*xxx_controller_serial_number* to eui.*xxx (NGUID)* in the entire ESXi environment. If you use the device identifier in any of your customer scripts, you must reflect this format change.

Verify Mapping Between Primary and Alternative Device Identifiers

Use the `esxcli storage core device uidmap list` command to verify the device identifiers. The output is similar to the following:

```
  esxcli storage core device uidmap list
eui.0000xyz.....
   Primary UID: eui.0000xyz.....
   Alternative Primary UIDs: t10.0000abc....
   Legacy UID: vml.0000000000766d68....
   Alternative Legacy UIDs: vml.000000000080906....
```

Upgrade Stateless ESXi Hosts with NGUID-only NVMe Devices to Version 7.0.x

If your environment contains stateless ESXi hosts of version 6.7 and earlier and includes NVMe devices that support only NGUID format, you use the present workflow to upgrade the hosts to version 7.0.x.

- Your environment contains stateless ESXi 6.7 or earlier hosts.
- The environment includes NVMe devices that support only NGUID format.

When upgrading your stateless hosts from version 6.7 and earlier to version 7.0.x, perform these steps to retain the storage configuration. If you perform the upgrade without following the instructions, all storage configurations captured in host profiles might not be retained across the upgrade. As a result, you might encounter host profile compliance failures after the upgrade.

1. Determine whether the host contains NGUID-only NVMe devices.
   a) Verify whether the vendor of the device is NVMe.

      Use the following command as an example.

      ```
      # esxcli storage core device list -d eui.f04xxxxxxxxx0000000100000001
      eui.f04xxxxxxxxx0000000100000001
      Display Name: Local NVMe Disk (eui.f04xxxxxxxxx0000000100000001)
      Has Settable Display Name: true
      Devfs Path: /vmfs/devices/disks/eui.f04bxxxxxxxxx0000000100000001
      Vendor: NVMe
      ```

The `Vendor: NVMe` line indicates that the device is NVMe.

b) Determine which HBA is connected to the NVMe device.

```
# esxcli storage core adapter device list
HBA    Device UID
------ --------------------------------
vmhba2 eui.f04xxxxxxxxx0000000100000001
```

c) Obtain the namespace information for the NVMe device using the HBA and the namespace ID.

```
# esxcli nvme device namespace get -A vmhba2 -n 1
Namespace Identify Info:
Namespace Size: 0xe8e088b0 Logical Blocks
Namespace Capacity: 0xe8e088b0 Logical Blocks
. . .
NVM Capacity: 0x1d1c1116000
Namespace Globally Unique Identifier: 0xf04xxxxxxxxx0000000100000001
IEEE Extended Unique Identifier: 0x0
```

In the output, for an NGUID-only NVMe device, the field `IEEE Extended Unique Identifier` contains 0 and `Namespace Globally Unique Identifier` contains a non-zero value.

2. To retain storage configurations captured in the host profile, perform these steps when upgrading a stateless host to 7.0.x.

a) Before the upgrade, store `esx.conf` in a persistent location.

For example, you can copy the `esx.conf` file to a VMFS datastore.

```
# cp /etc/vmware/esx.conf /vmfs/volumes/datastore1/
```

b) Upgrade the host.

After the upgrade, the host is not compliant with the profile and might remain in maintenance mode.

c) Apply the device settings for NGUID-only NVMe devices using new ID formats.

Run the following command from the host indicating the location of the `esx.conf` file.

```
# python ./usr/lib/vmware/nvme-nguid-support/bin/nguidApplySettings.pyc -l /vmfs/volumes/datastore1/
```

3. Copy the settings from the host and reset host customizations.

a) In the vSphere Client, click **Home** > **Policies and Profiles** > **Host Profiles**, and click the profile attached to the host.

b) Click **Configure tab** > **Copy Setting from Host** and select the host.

c) To reset customizations, navigate to the host and select **Host Profiles** > **Reset Host Customizations** from the right-click menu.

4. From the host's right-click menu, select **Host Profiles** > **Remediate**.

The host becomes compliant.

5. Reboot the host and exit the maintenance mode.

Upgrade the ESXi Host Without Retaining Storage Configurations

If you don't retain the storage configurations captured in the host profile, after you upgrade the host, you might encounter some compliance failures on the host. In this case, copy the settings from the host and reset host customizations.

Rename Storage Devices

The ESXi host assigns a display name to a storage device based on the storage type and manufacturer. You can change the display name of the device.

You cannot rename certain types of local devices.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. Select the device to rename and click **Rename**.
5. Change the device name to a friendly name.

Storage Rescan Operations

When you perform storage management tasks or make changes in the SAN configuration, you might need to rescan your storage.

When you perform VMFS datastore management operations, such as creating a VMFS datastore or RDM, adding an extent, and increasing or deleting a VMFS datastore, your host or the vCenter Server automatically rescans and updates your storage. You can disable the automatic rescan feature by turning off the Host Rescan Filter. See Turn Off Storage Filters.

In certain cases, you need to perform a manual rescan. You can rescan all storage available to your host or to all hosts in a folder, cluster, and data center.

If the changes you make are isolated to storage connected through a specific adapter, perform a rescan for this adapter.

Perform the manual rescan each time you make one of the following changes.

- Zone a new disk array on a SAN.
- Create new LUNs on a SAN.
- Change the path masking on a host.
- Reconnect a cable.
- Change CHAP settings (iSCSI only).
- Add or remove discovery or static addresses (iSCSI only).
- Add a single host to the vCenter Server after you have edited or removed from the vCenter Server a datastore shared by the vCenter Server hosts and the single host.

Important: If you rescan when a path is unavailable, the host removes the path from the list of paths to the device. The path reappears on the list as soon as it becomes available and starts working again.

Perform Storage Rescan

When you make changes in your SAN configuration, you might need to rescan storage. You can rescan all storage available to your ESXi host, cluster, or data center. If the changes you make are isolated to storage accessed through a specific host, perform the rescan for only this host.

1. In the vSphere Client object navigator, browse to a host, a cluster, a data center, or a folder that contains hosts.
2. From the right-click menu, select **Storage** > **Rescan Storage**.
3. Specify extent of rescan.

Option	Description
Scan for New Storage Devices	Rescan all adapters to discover new storage devices. If new devices are discovered, they appear in the device list.

Option	Description
Scan for New VMFS Volumes	Rescan all storage devices to discover new datastores that have been added since the last scan. Any new datastores appear in the datastore list.

Perform Adapter Rescan

When you make changes in your SAN configuration and these changes are isolated to storage accessed through a specific adapter on ESXi host, perform rescan for only this adapter.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter to rescan from the list.
4. Click the **Rescan Adapter** icon.

Change the Number of Scanned Storage Devices

The range of scanned LUN IDs for an ESXi host can be from 0 to 16,383. ESXi ignores LUN IDs greater than 16,383. The configurable `Disk.MaxLUN` parameter controls the range of scanned LUN ID range. The parameter has a default value of 1024.

The `Disk.MaxLUN` parameter also determines how many LUNs the SCSI scan code attempts to discover using individual INQUIRY commands if the SCSI target does not support direct discovery using REPORT_LUNS.

You can modify the `Disk.MaxLUN` parameter depending on your needs. For example, if your environment has a smaller number of storage devices with LUN IDs from 1 through 100, set the value to 101. As a result, you can improve device discovery speed on targets that do not support REPORT_LUNS. Lowering the value can shorten the rescan time and boot time. However, the time to rescan storage devices might also depend on other factors, including the type of the storage system and the load on the storage system.

In other cases, you might need to increase the value if your environment uses LUN IDs that are greater than 1023.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. In the Advanced System Settings table, select **Disk.MaxLUN** and click the **Edit** icon.
5. Change the existing value to the value of your choice, and click **OK**.
   The value you enter specifies the LUN ID that is after the last one you want to discover.
   For example, to discover LUN IDs from 1 through 100, set **Disk.MaxLUN** to 101.

Identifying Device Connectivity Problems

When your ESXi host experiences a problem while connecting to a storage device, the host treats the problem as permanent or temporary depending on certain factors.

Storage connectivity problems are caused by a variety of reasons. Although ESXi cannot always determine the reason for a storage device or its paths being unavailable, the host differentiates between a permanent device loss (PDL) state of the device and a transient all paths down (APD) state of storage.

Permanent Device Loss (PDL) A condition that occurs when a storage device permanently fails or is administratively removed or excluded. It is not expected to become available. When the device becomes permanently unavailable, ESXi receives appropriate sense codes or a login

	rejection from storage arrays, and is able to recognize that the device is permanently lost.
All Paths Down (APD)	A condition that occurs when a storage device becomes inaccessible to the host and no paths to the device are available. ESXi treats this as a transient condition because typically the problems with the device are temporary and the device is expected to become available again.

Connectivity Problems and vSphere High Availability

When the device enters the PDL or APD state, vSphere High Availability (HA) can detect connectivity problems and provide automated recovery for affected virtual machines on the ESXi host. vSphere HA uses VM Component Protection (VMCP) to protect virtual machines running on the host in the vSphere HA cluster against accessibility failures. For more information about VMCP and how to configure responses for datastores and virtual machines when the APD or PDL condition occurs, see the *vSphere Availability* documentation.

Detecting PDL Conditions

A storage device is considered to be in the permanent device loss (PDL) state when it becomes permanently unavailable to your ESXi host.

Typically, the PDL condition occurs when a device is unintentionally removed, or its unique ID changes, or when the device experiences an unrecoverable hardware error.

When the storage array determines that the device is permanently unavailable, it sends SCSI sense codes to the ESXi host. After receiving the sense codes, your host recognizes the device as failed and registers the state of the device as PDL. For the device to be considered permanently lost, the sense codes must be received on all its paths.

After registering the PDL state of the device, the host stops attempts to reestablish connectivity or to send commands to the device.

The vSphere Client displays the following information for the device:

- The operational state of the device changes to `Lost Communication`.
- All paths are shown as `Dead`.
- Datastores on the device are not available.

If no open connections to the device exist, or after the last connection closes, the host removes the PDL device and all paths to the device. You can disable the automatic removal of paths by setting the advanced host parameter `Disk.AutoremoveOnPDL` to 0.

If the device returns from the PDL condition, the host can discover it, but treats it as a new device. Data consistency for virtual machines on the recovered device is not guaranteed.

Note: When a device fails without sending appropriate SCSI sense codes or an iSCSI login rejection, the host cannot detect PDL conditions. In this case, the host continues to treat the device connectivity problems as APD even when the device fails permanently.

Permanent Device Loss and SCSI Sense Codes

The following VMkernel log example of a SCSI sense code indicates that the device is in the PDL state.

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

Permanent Device Loss and iSCSI

On iSCSI arrays with a single LUN per target, PDL is detected through iSCSI login failure. An iSCSI storage array rejects your host's attempts to start an iSCSI session with a reason `Target Unavailable`. As with the sense codes, this response must be received on all paths for the device to be considered permanently lost.

Permanent Device Loss and Virtual Machines

After registering the PDL state of the device, the host closes all I/O from virtual machines. vSphere HA can detect PDL and restart failed virtual machines.

Performing Planned Storage Device Removal

When a storage device is malfunctioning, you can avoid permanent device loss (PDL) conditions or all paths down (APD) conditions. Perform a planned removal and reconnection of a storage device.

Planned device removal is an intentional disconnection of a storage device. You might also plan to remove a device for such reasons as upgrading your hardware or reconfiguring your storage devices. When you perform an orderly removal and reconnection of a storage device, you complete a number of tasks.

Task	Description
Migrate virtual machines from the device you plan to detach.	*vCenter Server and Host Management*
Unmount the datastore deployed on the device.	See Unmount Datastores.
Detach the storage device.	See Detach Storage Devices.
For an iSCSI device with a single LUN per target, delete the static target entry from each iSCSI HBA that has a path to the storage device.	See Remove Dynamic or Static iSCSI Targets.
Perform any necessary reconfiguration of the storage device by using the array console.	See your vendor documentation.
Reattach the storage device.	See Attach Storage Devices.
Mount the datastore and restart the virtual machines.	See Mount Datastores.

Detach Storage Devices

Safely detach a storage device from your ESXi host.

- The device does not contain any datastores.
- No virtual machines use the device as an RDM disk.
- The device does not contain a diagnostic partition or a scratch partition.

You might need to detach the device to make it inaccessible to your host, when, for example, you perform a hardware upgrade on the storage side.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. Select the device to detach and click the **Detach** icon.

The device becomes inaccessible. The operational state of the device changes to Unmounted.

If multiple hosts share the device, detach the device from each host.

Attach Storage Devices

Reattach a storage device that you previously detached from the ESXi host.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. Select the detached storage device and click the **Attach** icon.

The device becomes accessible.

Recovering from PDL Conditions

An unplanned permanent device loss (PDL) condition occurs when a storage device becomes permanently unavailable without being properly detached from the ESXi host.

The following items in the vSphere Client indicate that the device is in the PDL state:

- The datastore deployed on the device is unavailable.
- Operational state of the device changes to Lost Communication.
- All paths are shown as Dead.
- A warning about the device being permanently inaccessible appears in the VMkernel log file.

To recover from the unplanned PDL condition and remove the unavailable device from the host, perform the following tasks.

Task	Description
Power off and unregister all virtual machines that are running on the datastore affected by the PDL condition.	See *vSphere Virtual Machine Administration*.
Unmount the datastore.	See Unmount Datastores.
Rescan all ESXi hosts that had access to the device. **Note:** If the rescan is not successful and the host continues to list the device, some pending I/O or active references to the device might still exist. Check for any items that might still have an active reference to the device or datastore. The items include virtual machines, templates, ISO images, raw device mappings, and so on.	See Perform Storage Rescan.

Handling Transient APD Conditions

A storage device is considered to be in the all paths down (APD) state when it becomes unavailable to your ESXi host for an unspecified time period.

The reasons for an APD state can be, for example, a failed switch or a disconnected storage cable.

In contrast with the permanent device loss (PDL) state, the host treats the APD state as transient and expects the device to be available again.

The host continues to retry issued commands in an attempt to reestablish connectivity with the device. If the host's commands fail the retries for a prolonged period, the host might be at risk of having performance problems. Potentially, the host and its virtual machines might become unresponsive.

To avoid these problems, your host uses a default APD handling feature. When a device enters the APD state, the host turns on a timer. With the timer on, the host continues to retry non-virtual machine commands for a limited time period only.

By default, the APD timeout is set to 140 seconds. This value is typically longer than most devices require to recover from a connection loss. If the device becomes available within this time, the host and its virtual machine continue to run without experiencing any problems.

If the device does not recover and the timeout ends, the host stops its attempts at retries and stops any non-virtual machine I/O. Virtual machine I/O continues retrying. The vSphere Client displays the following information for the device with the expired APD timeout:

- The operational state of the device changes to `Dead or Error`.
- All paths are shown as `Dead`.
- Datastores on the device are dimmed.

Even though the device and datastores are unavailable, virtual machines remain responsive. You can power off the virtual machines or migrate them to a different datastore or host.

If later the device paths become operational, the host can resume I/O to the device and end the special APD treatment.

Disable Storage APD Handling

The storage all paths down (APD) handling on your ESXi host is enabled by default. When it is enabled, the host continues to retry nonvirtual machine I/O commands to a storage device in the APD state for a limited time period. When the time period expires, the host stops its retry attempts and terminates any nonvirtual machine I/O. You can disable the APD handling feature on your host.

If you disable the APD handling, the host will indefinitely continue to retry issued commands in an attempt to reconnect to the APD device. This behavior might cause virtual machines on the host to exceed their internal I/O timeout and become unresponsive or fail. The host might become disconnected from vCenter Server.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. In the Advanced System Settings table, select the **Misc.APDHandlingEnable** parameter and click the `Edit` icon.
5. Change the value to 0.

If you disabled the APD handling, you can reenable it and set its value to 1 when a device enters the APD state. The internal APD handling feature turns on immediately and the timer starts with the current timeout value for each device in APD.

Change Timeout Limits for Storage APD

The timeout parameter controls how many seconds the ESXi host must retry the I/O commands to a storage device in an all paths down (APD) state. You can change the default timeout value.

The timeout period begins immediately after the device enters the APD state. After the timeout ends, the host marks the APD device as unreachable. The host stops its attempts to retry any I/O that is not coming from virtual machines. The host continues to retry virtual machine I/O.
By default, the timeout parameter on your host is set to 140 seconds. You can increase the value of the timeout if, for example, storage devices connected to your ESXi host take longer than 140 seconds to recover from a connection loss.

Note: If you change the timeout parameter after the device becomes unavailable, the change does not take effect for that particular APD incident.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. In the Advanced System Settings table, select the **Misc.APDTimeout** parameter and click the `Edit` icon.
5. Change the default value.
   You can enter a value between 20 and 99999 seconds.

Verify the Connection Status of a Storage Device on ESXi Host

Use the `esxcli` command to verify the connection status of a particular storage device.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. Run the `esxcli storage core device list -d=`*`device_ID`* command.
2. Review the connection status in the `Status:` area.
   - `on` - Device is connected.
   - `dead` - Device has entered the APD state. The APD timer starts.
   - `dead timeout` - The APD timeout has expired.
   - `not connected` - Device is in the PDL state.

Enable or Disable Locator LED on ESXi Storage Devices

Use the locator LED to identify specific storage devices, so that you can locate them among other devices. You can turn the locator LED on or off.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. From the list of storage devices, select one or more disks and enable or disable the locator LED indicator.

Option	Description
Enable	Click the **Turn On LED** icon.
Disable	Click the **Turn Off LED** icon.

Erase Storage Devices

Certain functionalities, such as vSAN or virtual flash resource, require that your ESXi host uses clean storage devices. You can erase an HHD or flash device and remove all existing data.

- Make sure that the host is in the connected state.

- Verify that the devices you plan to erase are not in use.
- Required privilege: **Host.Config.Storage**

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. Select one or more devices and click the **Erase Partitions** icon.
5. Verify that the partition information you are erasing is not critical.
6. Click **OK** to confirm your change.

Change Perennial Reservation Settings

You can adjust the perennial reservation setting on storage devices that are used as physical Raw Device Mappings (RDMs) in Windows Server Failover Clustering (WSFC) configurations.

Before marking a device as perennially reserved, make sure the device does not contain a VMFS datastore.

WSFC cluster nodes that are spread over several ESXi hosts require physical RDMs. The RDMs are shared among all hosts where cluster nodes run. The host with the active node holds persistent SCSI-3 reservations on all shared RDM devices. When the active node is running and devices are locked, no other host can write to the devices. If another participating host boots while the active node is holding the lock on the devices, the boot might take unusually long time because the host unsuccessfully attempts to contact the locked devices. The same issue might also affect rescan operations.

To prevent this problem, activate perennial reservation for all devices on the ESXi hosts where secondary WSFC nodes with RDMs reside. This setting informs the ESXi host about the permanent SCSI reservation on the devices, so that the host can skip the devices during the boot or storage rescan process.

If you later re-purpose the marked devices as VMFS datastores, remove the reservation to avoid unpredictable datastore behavior.

For information about WSFC clusters, see the *Setup for Windows Server Failover Clustering* documentation.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. From the list of storage devices, select the device and click one of the following icons.

Option	Description
Mark as Perennially Reserved	Mark the selected device as perennially reserved. **Note:** Repeat the procedure for each RDM device that is participating in the WSFC cluster.
Unmark as Perennially Reserved	Clear perennial reservation for the device that was previously marked.

The configuration is permanently stored with the ESXi host and persists across restarts.

You can also use the `esxcli` command to mark the devices participating in the WSFC cluster.

1. Mark the devices as perennially reserved.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=true
```

2. Verify that the device is perennially reserved.

   ```
   esxcli storage core device list -dnaa.id
   ```

   In the output of the `esxcli` command, search for the entry `Is Perennially Reserved: true`.
3. To remove the perennially reserved flag, run the following command.

   ```
   esxcli storage core device setconfig -dnaa.id--perennially-reserved=false
   ```

Working with Flash Devices

In addition to regular storage hard disk drives (HDDs), ESXi supports flash storage devices.

Unlike regular HDDs that are electromechanical devices containing moving parts, flash devices use semiconductors as their storage medium and have no moving parts. Typically, the flash devices are resilient and provide faster access to data.

To detect flash devices, ESXi uses an inquiry mechanism based on T10 standards. Check with your vendor whether your storage array supports the ESXi mechanism of flash device detection.

After the host detects the flash devices, you can use them for several tasks and functionalities.

If you use NVMe storage, enable the high-performance plug-in (HPP) to improve your storage performance. See VMware High Performance Plug-In and Path Selection Schemes.

For specifics about using NVMe storage with ESXi, see About VMware NVMe Storage.

Table 212: Using Flash Devices with ESXi

Functionality	Description
vSAN	vSAN requires flash devices. For more information, see the *Administering VMware vSAN* documentation.
VMFS Datastores	Create VMFS datastores on flash devices. Use the datastores for the following purposes: • Store virtual machines. Certain guest operating systems can identify virtual disks stored on these datastores as flash virtual disks. • Allocate datastore space for the ESXi host swap cache. See Configure Host Cache with VMFS Datastore.
Virtual Flash Resource (VFFS)	If required by your vendor, set up a virtual flash resource and use it for I/O caching filters. See Filtering Virtual Machine I/O.

Flash Devices and Virtual Machines

Guest operating systems can identify virtual disks that reside on flash-based datastores as flash virtual disks.

Guest operating systems can use standard inquiry commands such as SCSI VPD Page (B1h) for SCSI devices and ATA IDENTIFY DEVICE (Word 217) for IDE devices.

For linked clones, native snapshots, and delta-disks, the inquiry commands report the virtual flash status of the base disk.

Operating systems can detect that a virtual disk is a flash disk under the following conditions:

- Detection of flash virtual disks is supported on VMs with virtual hardware version 8 or later.
- Devices backing a shared VMFS datastore must be marked as flash on all hosts.
- If the VMFS datastore includes several device extents, all underlying physical extents must be flash-based.

Marking Storage Devices

You can mark storage devices on an ESXi host as local flash devices.

When you configure vSAN or set up a virtual flash resource, your storage environment must include local flash devices.

However, ESXi might not recognize certain storage devices as flash devices when their vendors do not support automatic flash device detection. In other cases, certain devices might not be detected as local, and ESXi marks them as remote. When devices are not recognized as the local flash devices, they are excluded from the list of devices offered for vSAN or virtual flash resource. Marking these devices as local flash makes them available for vSAN and virtual flash resource.

Mark Storage Devices as Flash

If ESXi does not recognize its devices as flash, mark them as flash devices.

Verify that the device is not in use.

ESXi does not recognize certain devices as flash when their vendors do not support automatic flash disk detection. The Drive Type column for the devices shows HDD as their type.

CAUTION: Marking the HDD devices as flash might deteriorate the performance of datastores and services that use them. Mark the devices only if you are certain that they are flash devices.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. From the list of storage devices, select one or several HDD devices and click the **Mark as Flash Disk** ( ) icon.
5. Click **Yes** to save your changes.

The type of the devices changes to flash.
If the flash device that you mark is shared among multiple hosts, make sure that you mark the device from all hosts that share the device.

Mark Storage Devices as Local

ESXi enables you to mark devices as local. This action is useful in cases when ESXi is unable to determine whether certain devices are local.

- Make sure that the device is not shared.
- Power off virtual machines that reside on the device and unmount an associated datastore.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. From the list of storage devices, select one or several remote devices and click the **Mark as Local** icon.
5. Click **Yes** to save your changes.

Monitor Flash Devices

You can monitor certain critical flash device parameters, including `Media Wearout Indicator`, `Temperature`, and `Reallocated Sector Count`, from an ESXi host.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Use the `esxcli` command to monitor flash devices.

Display the flash device statistics by running the following command:

`esxcli storage core device smart get -d=`*`flash device_ID`*

Best Practices for Flash Devices

Follow these best practices when you use flash devices in vSphere environment.

- Use flash devices approved by the *VMware Compatibility Guide*.
- Make sure to use the latest firmware with flash devices. Frequently check with your storage vendors for any updates.
- Carefully monitor how intensively you use the flash device and calculate its estimated lifetime. The lifetime expectancy depends on how actively you continue to use the flash device. See Estimate Lifetime of Flash Devices.
- If you use NVMe devices for storage, enable the high-performance plug-in (HPP) to improve your storage performance. For specifics of using the NVMe devices, see VMware High Performance Plug-In and Path Selection Schemes

Estimate Lifetime of Flash Devices

When working with flash devices, monitor how actively you use them and calculate their estimated lifetime.

Note the number of days passed since the last reboot of your ESXi host. For example, ten days.

Typically, storage vendors provide reliable lifetime estimates for a flash device under ideal conditions. For example, a vendor might guarantee a lifetime of 5 years under the condition of 20 GB writes per day. However, the more realistic life expectancy of the device depends on how many writes per day your ESXi host actually generates. Follow these steps to calculate the lifetime of the flash device.

1. Obtain the total number of blocks written to the flash device since the last reboot.

   Run the `esxcli storage core device stats get -d=device_ID` command. For example:

   ```
   ~ # esxcli storage core device stats get -d t10.xxxxxxxxxxxxxxx
    Device: t10.xxxxxxxxxxxxxxx
    Successful Commands: xxxxxxx
    Blocks Read: xxxxxxxx
    Blocks Written: 629145600
    Read Operations: xxxxxxxx
   ```

   The Blocks Written item in the output shows the number of blocks written to the device since the last reboot. In this example, the value is 629,145,600. After each reboot, it resets to 0.

2. Calculate the total number of writes and convert to GB.

   One block is 512 bytes. To calculate the total number of writes, multiply the Blocks Written value by 512, and convert the resulting value to GB.

   In this example, the total number of writes since the last reboot is approximately 322 GB.

3. Estimate the average number of writes per day in GB.

   Divide the total number of writes by the number of days since the last reboot.

   If the last reboot was ten days ago, you get 32 GB of writes per day. You can average this number over the time period.

4. Estimate lifetime of your device by using the following formula:

   `vendor provided number of writes per day` times *`vendor provided life span`* divided by *`actual average number of writes per day`*

   For example, if your vendor guarantees a lifetime of 5 years under the condition of 20 GB writes per day, and the actual number of writes per day is 30 GB, the life span of your flash device will be approximately 3.3 years.

About Virtual Flash Resource

You can aggregate local flash devices on an ESXi host into a single virtualized caching layer called virtual flash resource.

When you set up the virtual flash resource, you create a new file system, Virtual Flash File System (VFFS). VFFS is a derivative of VMFS, which is optimized for flash devices and is used to group the physical flash devices into a single caching resource pool. As a non-persistent resource, it cannot be used to store virtual machines.

After you set up the virtual flash resource, you can use it for I/O caching filters. See Filtering Virtual Machine I/O.

Considerations for Virtual Flash Resource

When you configure a virtual flash resource, several considerations apply.

- You can have only one virtual flash resource on a single ESXi host. The virtual flash resource is managed at the host's level.
- You cannot use the virtual flash resource to store virtual machines. Virtual flash resource is a caching layer only.
- You can use only local flash devices for the virtual flash resource.
- You can create the virtual flash resource from mixed flash devices. All device types are treated equally and no distinction is made between SAS, SATA, or PCI express connectivity. When creating the resource from mixed flash devices, make sure to group similar performing devices together to maximize performance.
- You cannot use the same flash devices for the virtual flash resource and vSAN. Each requires its own exclusive and dedicated flash device.

Set Up Virtual Flash Resource

You can set up a virtual flash resource or add capacity to existing virtual flash resource.

To set up a virtual flash resource, you use local flash devices connected to your host or host cluster. To increase the capacity of your virtual flash resource, you can add more devices, up to the maximum number indicated in the *Configuration Maximums* documentation. An individual flash device must be exclusively allocated to the virtual flash resource. No other vSphere functionality, such as vSAN or VMFS, can share the device with the virtual flash resource.

1. In the vSphere Client, navigate to the host.
2. Click the **Configure** tab.
3. Under **Virtual Flash**, click **Virtual Flash Resource Management**.
4. Click one of the following options.

Option	Description
Add Capacity	If you are creating the virtual flash resource on an individual host.
Add Capacity on Cluster	If you are creating the virtual flash resource on a cluster.

5. From the list of available entities, select one or more to use for the virtual flash resource and click **OK**.

   If your flash devices do not appear on the list, see Marking Storage Devices.

Option	Description
Local VMware Disk	Select any combination of unclaimed flash devices. ESXi creates the VFFS volume on one of the devices and then extends the volume on the rest of the devices. The system configures the virtual flash resource on the entire VFFS volume. If a VFFS volume exists on your host, you cannot select any unclaimed devices without first selecting the existing VFFS volume.
volume ID **- Configure using the existing VFFS volume extents**	If you previously created a VFFS volume on one of the host's flash devices using the `vmkfstools` command, the volume also appears on the list of eligible entities. You can select just

Option	Description
	this volume for the virtual flash resource. Or combine it with the unclaimed devices. ESXi uses the existing VFFS volume to extend it over other devices.

The virtual flash resource is created. The Device Backing area lists all devices that you use for the virtual flash resource. Use the virtual flash resource for I/O caching filters developed through vSphere APIs for I/O Filtering. See Using Flash Storage Devices with Cache I/O Filters.

You can increase the capacity by adding more flash devices to the virtual flash resource.

Remove Virtual Flash Resource

You might need to remove a virtual flash resource deployed on local flash devices connected to the ESXi host. Removing the virtual flash resource frees the devices for other services.

- Verify that the virtual flash resource is not used for I/O filters.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Virtual Flash**, click **Virtual Flash Resource Management** and click **Remove All**.

After you remove the virtual flash resource and erase the flash device, the device is available for other operations.

Set Alarm for Virtual Flash Use

Set an alarm to indicate when the use of a virtual flash resource on your ESXi host exceeds specified threshold.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. Select the setting to change and click the **Edit** button.

Parameter	Description
VFLASH.ResourceUsageThreshold	The system triggers the `Host vFlash resource usage` alarm when a virtual flash resource use exceeds the threshold. The default threshold is 80%. You can change the threshold to an appropriate value. The alarm is cleared when the virtual flash resource use drops below the threshold.

5. Click **OK**.

Configure Host Cache with VMFS Datastore

Enable your ESXi host to swap to the host cache. You can also change the amount of space allocated for the host cache.

Create a VMFS datastore using flash devices as backing. See Create a VMFS Datastore.

Your ESXi hosts can use a portion of a flash-backed storage entity as a swap cache shared by all virtual machines.

The host-level cache is made up of files on a low-latency disk that ESXi uses as a write-back cache for virtual machine swap files. All virtual machines running on the host share the cache. Host-level swapping of virtual machine pages makes the best use of potentially limited flash device space.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Host Cache Configuration**.
4. Select the flash datastore in the list and click the **Edit** icon.
5. Allocate appropriate space for host cache.
6. Click **OK**.

Keeping Flash Disks VMFS-Free

If you use the auto-partitioning boot option when installing or auto-deploying ESXi, the auto-partitioning option creates a VMFS datastore on your host's local storage. In certain cases, you need to keep your local storage flash disks unformatted.

By default, auto-partitioning deploys VMFS file systems on any unused local storage disks on your host, including flash disks.

However, a flash disk formatted with VMFS becomes unavailable for such features as virtual flash and vSAN. Both features require an unformatted flash disk and neither can share the disk with any other file system.

To ensure that auto-partitioning does not format the flash disk with VMFS, use the following boot options when you install ESXi or boot the ESXi host for the first time:

- `autoPartition=TRUE`
- `skipPartitioningSsds=TRUE`

If you use Auto Deploy, set these parameters on a reference ESXi host.

1. In the vSphere Client, navigate to the host to use as a reference host and click the **Configure** tab.
2. Click **System** to open the system options, and click **Advanced System Settings**.
3. Set the following items.

Parameter	Value
VMkernel.Boot.autoPartition	True
VMkernel.Boot.skipPartitioningSsds	True

4. Reboot the host.

If flash disks that you plan to use with the virtual flash resource and vSAN already have VMFS datastores, remove the datastores.

About VMware NVMe Storage

Non-Volatile Memory (NVM) storage devices that use persistent memory have become increasingly popular in data centers. NVM Express (NVMe) is a standardized protocol designed specifically for high-performance multi-queue communication with NVM devices. ESXi supports the NVMe protocol to connect to local and networked storage devices.

VMware NVMe Concepts

Before you begin working with NVMe storage in the ESXi environment, you can familiarize yourself with basic NVMe concepts.

NVM Express (NVMe)

NVMe is a method for connecting and transferring data between a host and a target storage system. NVMe is designed for use with faster storage media equipped with non-volatile memory, such as flash devices. This type of storage can achieve low latency, low CPU usage, and high performance, and generally serves as an alternative to SCSI storage.

NVMe Transports

The NVMe storage can be directly attached to a host using a PCIe interface or indirectly through different fabric transports. VMware NVMe over Fabrics (NVMe-oF) provides a distance connectivity between a host and a target storage device on a shared storage array.

The following types of transports for NVMe currently exist. For more information, see Requirements and Limitations of VMware NVMe Storage.

NVMe Transport	ESXi Support
NVMe over PCIe	Local storage.
NVMe over RDMA	Shared NVMe-oF storage. With the RoCE v2 technology.
NVMe over Fibre Channel (FC-NVMe)	Shared NVMe-oF storage.
NVME over TCP	Shared NVMe-oF storage.

NVMe Namespaces

In the NVMe storage array, a namespace is a storage volume backed by some quantity of non-volatile memory. In the context of ESXi, the namespace is analogous to a storage device, or LUN. After your ESXi host discovers the NVMe namespace, a flash device that represents the namespace appears on the list of storage devices in the vSphere Client. You can use the device to create a VMFS datastore and store virtual machines.

NVMe Controllers

A controller is associated with one or several NVMe namespaces and provides an access path between the ESXi host and the namespaces in the storage array. To access the controller, the host can use two mechanisms, controller discovery and controller connection. For information, see Add Controller for NVMe over Fabrics.

Controller Discovery

With this mechanism, the ESXi host first contacts a discovery controller. The discovery controller returns a list of available controllers. After you select a controller for your host to access, all namespaces associated with this controller become available to your host.

Controller Connection

Your ESXi host connects to the controller that you specify. All namespaces associated with this controller become available to your host.

NVMe Subsystem

Generally, an NVMe subsystem is a storage array that might include several NVMe controllers, several namespaces, a non-volatile memory storage medium, and an interface between the controller and non-volatile memory storage medium. The subsystem is identified by a subsystem NVMe Qualified Name (NQN).

VMware High-Performance Plug-in (HPP)	By default, the ESXi host uses the HPP to claim the NVMe-oF targets. When selecting physical paths for I/O requests, the HPP applies an appropriate Path Selection Scheme (PSS). For information about the HPP, see VMware High Performance Plug-In and Path Selection Schemes. To change the default path selection mechanism, see Change the Path Selection Policy.

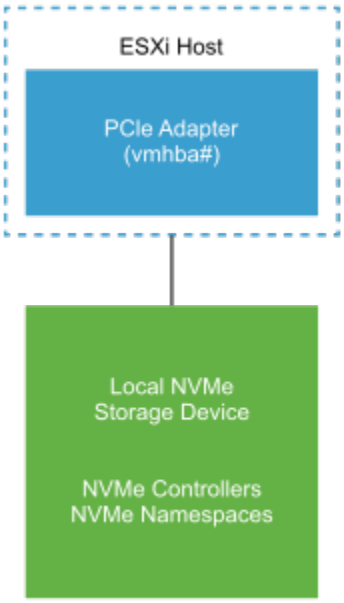
Basic VMware NVMe Architecture and Components

ESXi supports local NVMe over PCIe storage and shared NVMe-oF storage, such as NVMe over Fibre Channel, NVMe over RDMA (RoCE v2) and NVMe over TCP.

In NVMe-oF environments, targets can present namespaces, equivalent to LUNs in SCSI, to a host in active/active or asymmetric access modes. ESXi is able to discover and use namespaces presented in either way. ESXi internally emulates NVMe-oF targets as SCSI targets and presents them as active/active SCSI targets or implicit ALUA SCSI targets.

VMware NVMe over PCIe

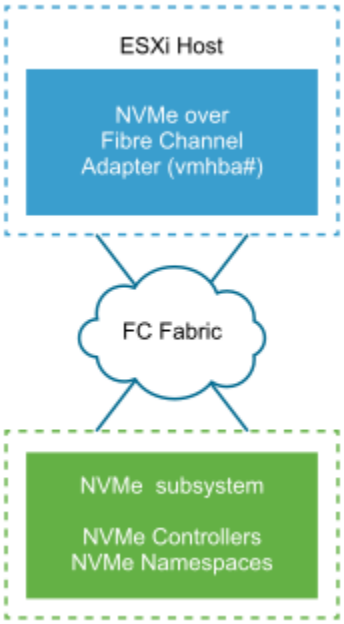
In this configuration, your ESXi host uses a PCIe storage adapter to access one or more local NVMe storage devices. After you install the adapter on the host, the host discovers available NVMe devices, and they appear in the list of storage devices in the vSphere Client.



VMware NVMe over FC

This technology maps NVMe onto the Fibre Channel protocol to enable the transfer of data and commands between a host computer and a target storage device. This transport can use existing Fibre Channel infrastructure upgraded to support NVMe.

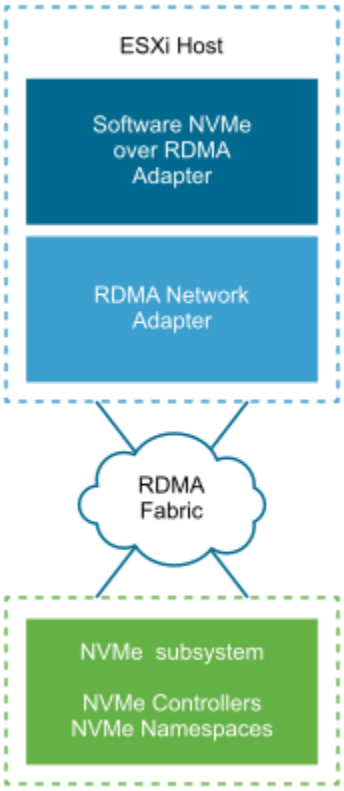
To access the NVMe over Fibre Channel storage, install a Fibre Channel storage adapter that supports NVMe on your ESXi host. You do not need to configure the adapter. It automatically connects to an appropriate NVMe subsystem and discovers all shared NVMe storage devices that it can reach. You can later reconfigure the adapter and disconnect its controllers or connect other controllers that were not available during the host boot. For more information, see Add Controller for NVMe over Fabrics.



NVMe over RDMA (RoCE v2)

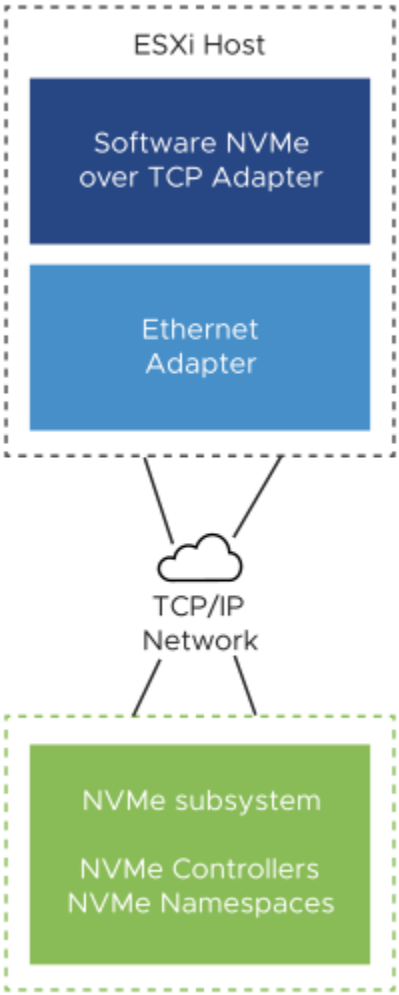
This technology uses a remote direct memory access (RDMA) transport between two systems on the network. The transport enables data exchange in the main memory bypassing the operating system or the processor of either system. ESXi supports RDMA over Converged Ethernet v2 (RoCE v2) technology, which enables a remote direct memory access over an Ethernet network.

To access storage, the ESXi host uses an RDMA network adapter installed on your host and a software NVMe over RDMA storage adapter. You must configure both adapters to use them for storage discovery. For more information, see Configure Adapters for NVMe over RDMA (RoCE v2) Storage.



NVMe over TCP

This technology uses Ethernet connections between two systems. To access storage, the ESXi host uses a network adapter installed on your host and a software NVMe over TCP storage adapter. You must configure both adapters to use them for storage discovery. For more information, see Configure Adapters for NVMe over TCP Storage.



Requirements and Limitations of VMware NVMe Storage

When you use the NVMe technology with VMware, follow specific guidelines and requirements.

Requirements for NVMe over PCIe

Your ESXi storage environment must include the following components:

- Local NVMe storage devices.
- Compatible ESXi host.
- Hardware NVMe over PCIe adapter. After you install the adapter, your ESXi host detects it and displays in the vSphere Client as a storage adapter (vmhba) with the protocol indicated as PCIe. You do not need to configure the adapter.

Requirements for NVMe over RDMA (RoCE v2)

- NVMe storage array with NVMe over RDMA (RoCE v2) transport support.
- Compatible ESXi host.
- Ethernet switches supporting a lossless network.
- Network adapter that supports RDMA over Converged Ethernet (RoCE v2). To configure the adapter, see View RDMA Network Adapters.

- Software NVMe over RDMA adapter. This software component must be enabled on your ESXi host and connected to an appropriate network RDMA adapter. For information, see Enable NVMe over RDMA or NVMe over TCP Software Adapters.
- NVMe controller. You must add a controller after you configure a software NVMe over RDMA adapter. See Add Controller for NVMe over Fabrics.

Requirements for NVMe over Fibre Channel

- Fibre Channel storage array that supports NVMe. For information, see Using ESXi with Fibre Channel SAN.
- Compatible ESXi host.
- Hardware NVMe adapter. Typically, it is a Fibre Channel HBA that supports NVMe. When you install the adapter, your ESXi host detects it and displays in the vSphere Client as a standard Fibre Channel adapter (vmhba) with the storage protocol indicated as NVMe. You do not need to configure the hardware NVMe adapter to use it.
- NVMe controller. You do not need to configure the controller. After you install the required hardware NVMe adapter, it automatically connects to all targets and controllers that are reachable at the moment. You can later disconnect the controllers or connect other controllers that were not available during the host boot. See Add Controller for NVMe over Fabrics.

Requirements for NVMe over TCP

- NVMe storage array with NVMe over TCP transport support.
- Compatible ESXi host.
- An ethernet adapter.
- Software NVMe over TCP adapter. This software component must be enabled on your ESXi host and connected to an appropriate network adapter. For more information, see Enable NVMe over RDMA or NVMe over TCP Software Adapters.
- NVMe controller. You must add a controller after you configure a software NVMe over TCP adapter. See Add Controller for NVMe over Fabrics.

VMware NVMe over Fabrics Shared Storage Support

In the ESXi environment, the NVMe storage devices appear similar to SCSI storage devices, and can be used as shared storage. Follow these rules when using the NVMe-oF storage.

- Do not mix transport types to access the same namespace.
- Make sure that active paths are presented to the host. The namespaces cannot be registered until the active path is discovered.

Shared Storage Functionality	SCSI over Fabric Storage	NVMe over Fabric Storage
RDM	Supported	Not supported
Core dump	Supported	Not supported
SCSI-2 reservations	Supported	Not supported
Clustered VMDK	Supported	Not supported
Shared VMDK with multi-writer flag	Supported	Supported In vSphere 7.0 Update 1 and later. For more information, see the Knowledge Base article.
Virtual Volumes	Supported	Not supported
Hardware acceleration with VAAI plug-ins	Supported	Not supported

Shared Storage Functionality	SCSI over Fabric Storage	NVMe over Fabric Storage
Default MPP	NMP	HPP (NVMe-oF targets cannot be claimed by NMP)
Limits	LUNs=1024, Paths=4096	Namespaces=32, Paths=128 (maximum 4 paths per namespace in a host)

Configuring Lossless Ethernet for NVMe over RDMA

NVMe over RDMA in ESXi requires a lossless Ethernet network to operate efficiently.

To establish lossless networks, you can select one of the available QoS settings.

Enabling Global Pause Flow Control

In this network configuration, ensure global pause flow control is enabled on the network switch ports. Also, ensure that RDMA capable NICs in the host auto-negotiate to the correct flow control automatically.

To check flow control, run the following commands.

```
#esxcli network nic get -n vmnicX
   Pause RX: true
   Pause TX: true
```

If the above command options are not set to true, run the following command.

```
#esxcli network nic pauseParams set -r true -t true -n vmnicX
```

Enabling Priority Flow Control

For RoCE traffic to be lossless, you must configure the PFC priority value to 3 in the physical switch and hosts. You can configure the PFC in the ESXi host in two ways:

- Automatic Configuration. Starting ESXi 7.0, you can apply DCB PFC configuration automatically on the host RNIC, if the RNIC driver supports DCB and DCBx.
  You can verify the current DCB settings by running the following command.
  ```
  #esxcli network nic dcb status get -n vmnicX
  ```
- Manual configuration. In some cases, the RNIC drivers provide a method to manually configure the DCB PFC using driver specific parameters. To use this method, see vendor specific driver documentation. For example,in Mellanox ConnectX-4/5 driver, you can set the PFC priority value to 3 by running the following command and reboot the host.
  ```
  #esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08"
  ```

Enabling DSCP based PFC

DSCP based PFC is another way to configure lossless network. In physical switches and hosts, you must set the DSCP value to 26. To use this option, see vendor specific driver documentation. For example, in Mellanox ConnectX-4/5 driver, you can set the DSCP tag value to 26 by running the following commands.

- Enable PFC and DSCP trust mode
  ```
  #esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08 trust_state=2"
  ```
- Set DSCP value to 26
  ```
  #esxcli system module parameters set -m nmlx5_rdma -p "dscp_force=26"
  ```
- Verify parameters to check to confirm if settings are correct and set.
  ```
  esxcli system module parameters list -m nmlx5_core | grep 'trust_state\|pfcrx\|pfctx'
  ```
- Reboot the host

Configure Adapters for NVMe over RDMA (RoCE v2) Storage

The adapter configuration process on the ESXi host involves setting up VMkernel binding for an RDMA network adapter, and then enabling a software NVMe over RDMA adapter.

The following video walks you through the steps of configuring NVMe over RDMA adapters.

After you enable the software NVMe over RDMA adapter, add NVMe controllers, so that the host can discover the NVMe targets. See Add Controller for NVMe over Fabrics.

View RDMA Network Adapters

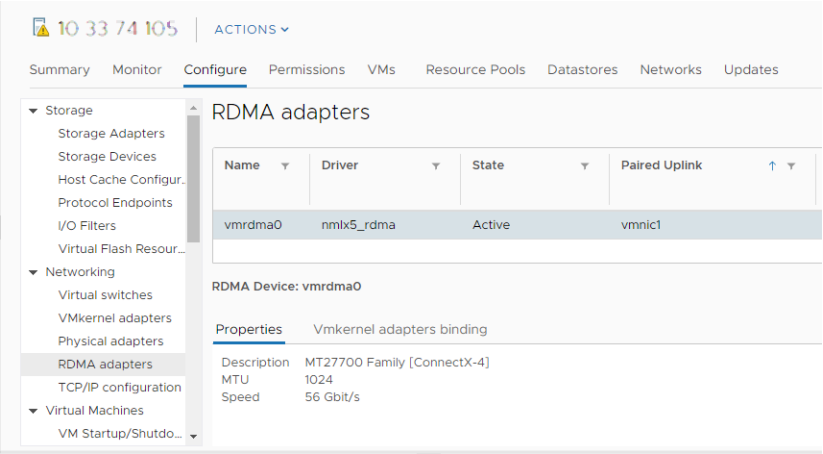
After you install a network adapter that supports RDMA (RoCE v2) on your ESXi host, use the vSphere Client to review the RDMA adapter and a physical network adapter.

1. On your ESXi host, install an adapter that supports RDMA (RoCE v2), for example, Mellanox Technologies MT27700 Family ConnectX-4.

   The host discovers the adapter and the vSphere Client displays its two components, an RDMA adapter and a physical network adapter.

2. In the vSphere Client, verify that the RDMA adapter is discovered by your host.
   a) Navigate to the host.
   b) Click the **Configure** tab.
   c) Under **Networking**, click **RDMA adapters**.

      In this example, the RDMA adapter appears on the list as `vmrdma0`. The **Paired Uplink** column displays the network component as the `vmnic1` physical network adapter.



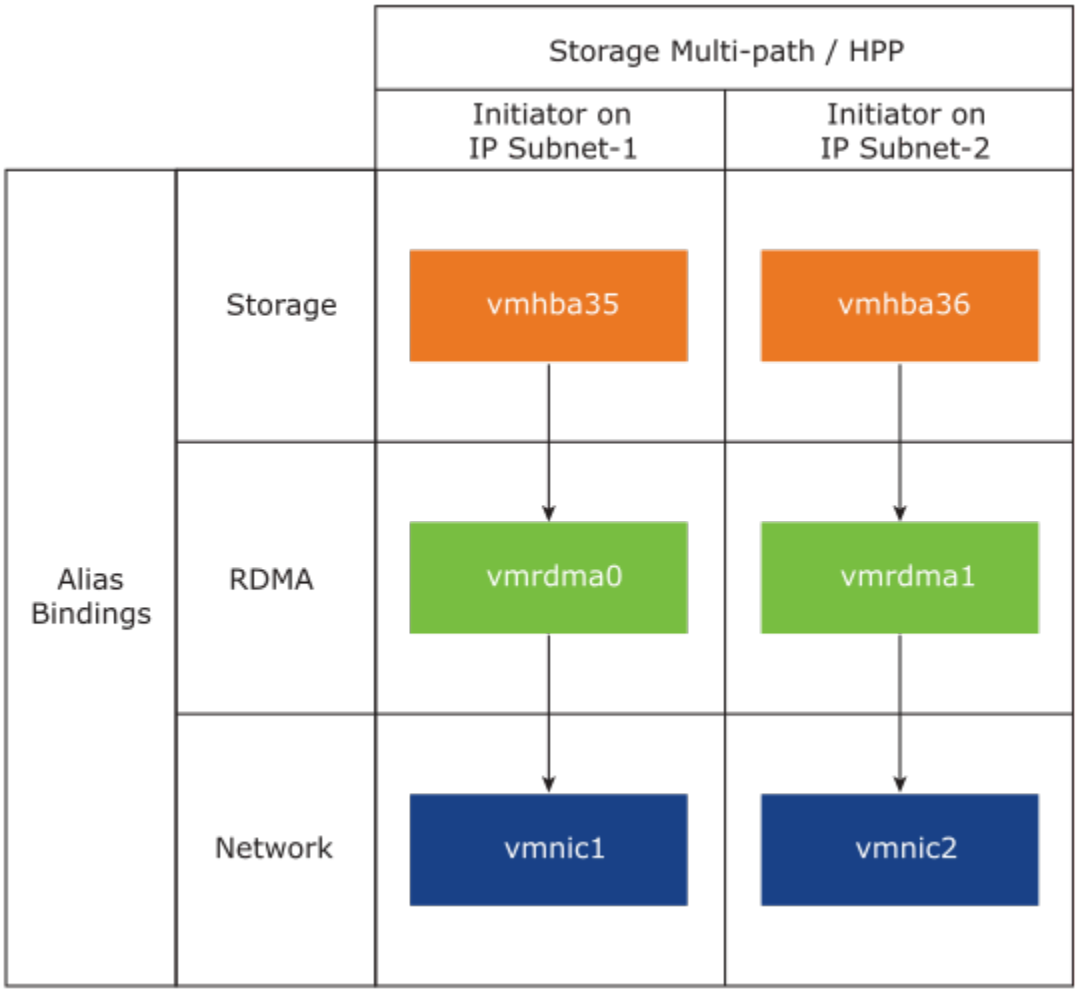
   d) To verify the description of the adapter, select the RDMA adapter from the list, and click the **Properties** tab.

You can now create the software NVMe over RDMA adapter.

Configure VMkernel Binding for the RDMA Adapter

Port binding for NVMe over RDMA involves creating a switch and connecting the physical network adapter and the VMkernel adapter to the switch. Through this connection, the RDMA adapter becomes bound to the VMkernel adapter. In the configuration, you can use a vSphere standard switch or a vSphere distributed switch.

The following diagram displays the port binding for the NVMe over RDMA adapter.

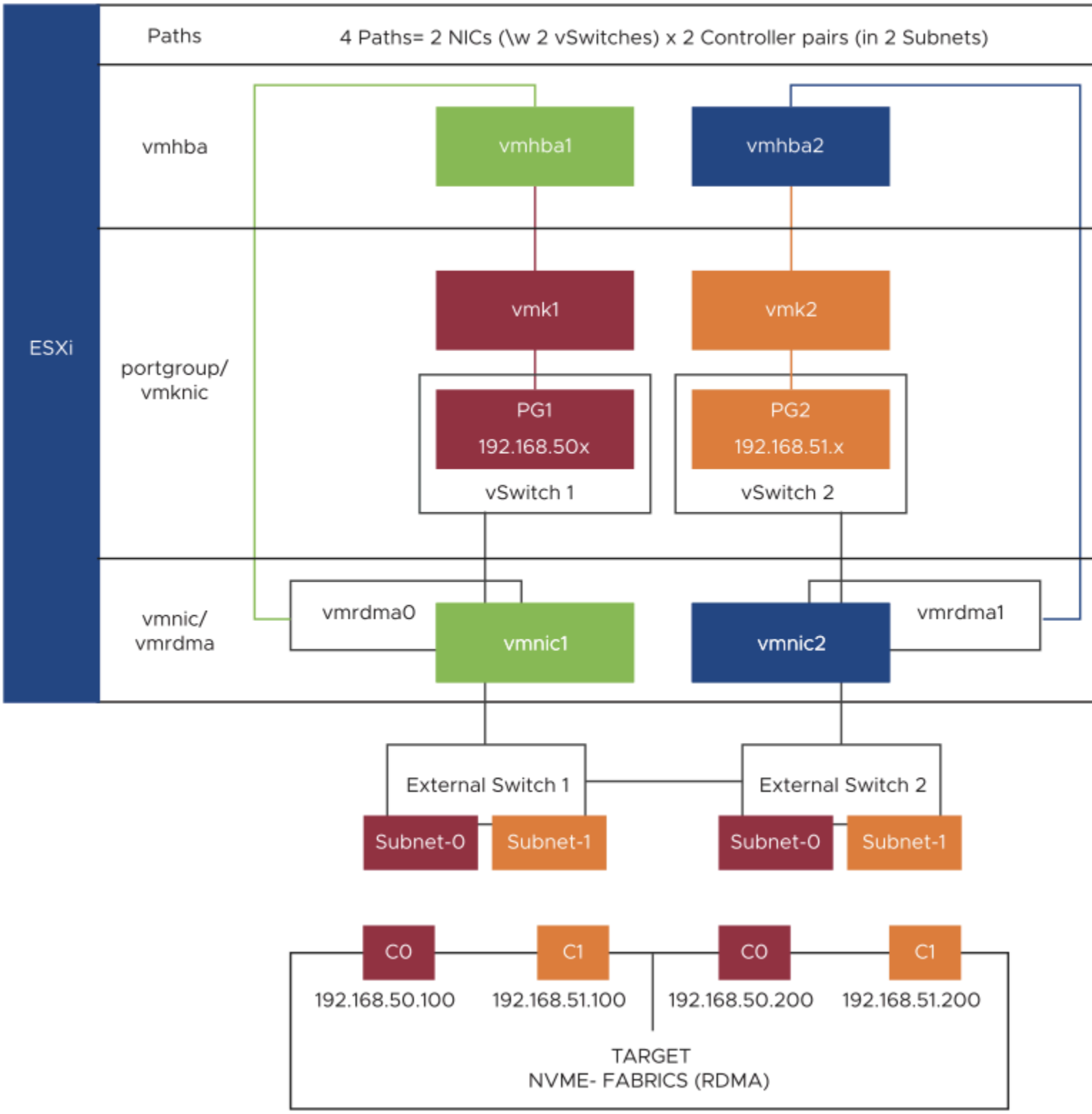


For more information about creating switches, see *Create a vSphere Standard Switch* or *Create a vSphere Distributed Switch* in the *vSphere Networking* documentation.

Example of Network Topology with NVMe over RDMA

In this example, two vSphere standard switches and two uplinks (RDMA capable NICs) provide high availability. They connect to two controller pairs in two subnets.

HA with Multiple vSwitches and Multiple Uplinks (RNICs)



Configure VMkernel Binding with a vSphere Standard Switch

You can configure VMkernel port binding for the RDMA adapter using a vSphere standard switch and one uplink per switch. Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter.

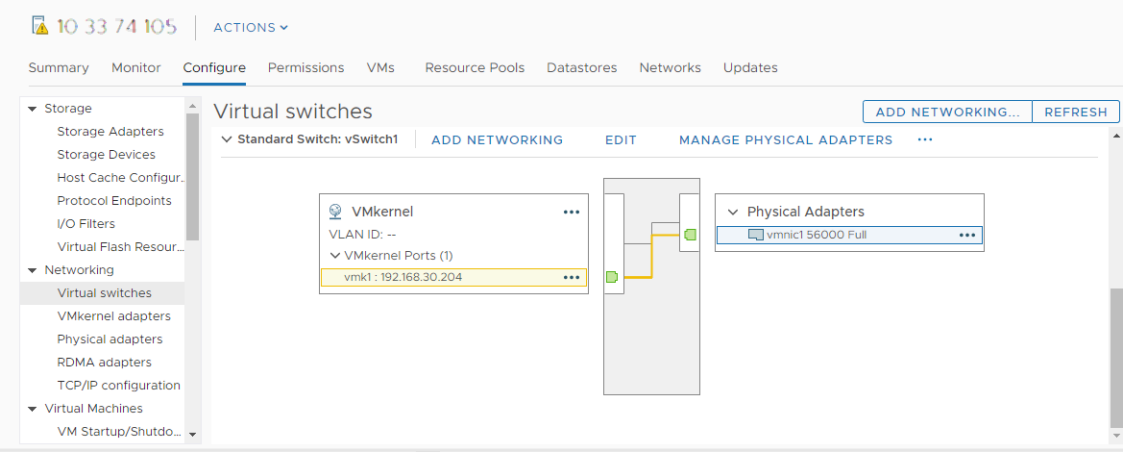
1. Create a vSphere standard switch with a VMkernel adapter and the network component.
   a) In the vSphere Client, select your host and click the **Networks** tab.
   b) Click **Actions** > **Add Networking**.
   c) Select **VMkernel Network Adapter** and click **NEXT**.
   d) Select **New standard switch** and click **NEXT**.
   e) Under **Assigned adapters**, click **+**.

      The list of available physical adapters is displayed.
   f) Select the required physical adapter `vmnic`, and click **OK**.

      Note: Ensure to select the physical network adapter that corresponds to the RDMA adapter. To see the association between the RDMA adapter `vmrdma`, and the physical network adapter `vmnic`, see View RDMA Network Adapters.
   g) Under **VMkernel port settings**, enter the required values.

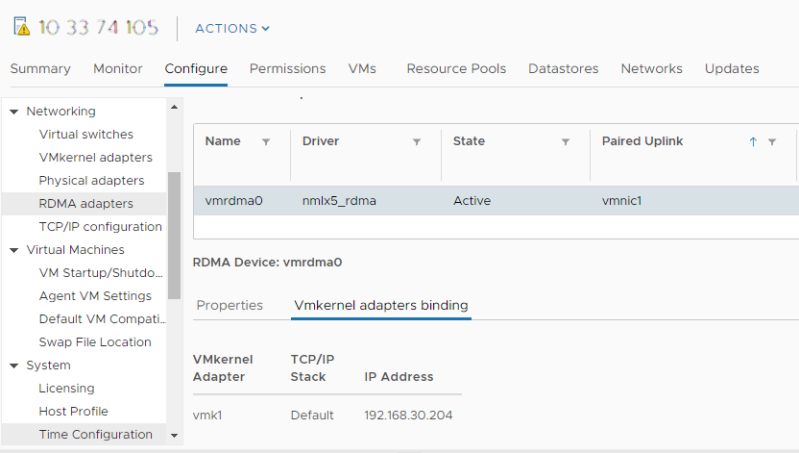
      If you are using VLAN for the storage path, enter the VLAN ID.
   h) In the **IP settings** list, enter the VMkernel IPv4 settings.
   i) Under Available services, select **NVMe over RDMA**.
2. Verify that your switch is correctly configured.
   a) On the **Configure** tab, select **Virtual switches** under **Networking**.
   b) Expand the switch and verify its configuration.

      The illustration shows that the physical network adapter and the VMkernel adapter are connected to the vSphere standard switch. Through this connection, the RDMA adapter is bound to the VMkernel adapter.



3. Verify the configuration of the VMkernel binding for the RDMA adapter.
   a) Under **Networking** list, click **RDMA adapters**, and select the RDMA adapter from the list.
   b) Click the **VMkernel adapters binding** tab and verify that the associated VMkernel adapter appears on the page.

      In this example, the `vmrdma0` RDMA adapter is paired to the `vmnic1` network adapter and is connected to the `vmk1` VMkernel adapter.



Configure VMkernel Binding with a vSphere Standard Switch and NIC Teaming

You can configure VMkernel port binding for the RDMA adapter using a vSphere standard switch with the NIC teaming configuration. You can use NIC teaming to achieve network redundancy. You can configure two or more network adapters (NICs) as a team for high availability and load balancing.

1. Create a vSphere standard switch with a VMkernel adapter and the network component with the NIC teaming configuration.
   a) In the vSphere Client, select your host and click **Networks** tab.
   b) Click **Actions** > **Add Networking**.
   c) Select **VMkernel Network Adapter** and click **NEXT**.
   d) Select **New standard switch** and click **NEXT**.
   e) Under **Assigned adapters**, click **+**.

      A list of available physical adapters is displayed.
   f) Select the required physical adapter `vmnic`, and add it under **Active adapters**.
   g) Select another physical adapter `vmnic`, and add it under **Unused adapters**.
   h) Under **VMkernel port settings**, enter the required values.

      If you are using VLAN for the storage path, enter the VLAN ID.
   i) In the **IP settings** list, specify VMkernel IPv4 settings.
   j) Under Available services, select **NVMe over RDMA**.

   Repeat step 1 to configure an existing standard switch.

2. Configure your switch for NIC teaming configuration.
   a) Click the **Configure** tab, and select **Virtual switches** under **Networking**.
   b) Select the appropriate VMkernel adapter.
   c) From the right-click menu, click **Edit Settings**.
   d) Select **Teaming and Failover**.
   e) Under **Active adapters**, move the required physical adapter `vmnic`.
   f) Under **Standby adapters** > **Failover order**, move the other physcial adapters.
   g) Set appropriate load balancing and other properties.
   h) Repeat the steps to configure additional VMkernel adapters.
3. Repeat steps 1 and 2 to add and configure additional set of teamed `rnic`s. To verify if the adapter is configured, click the **Configure** tab and select **VMkernel adapters**

Configure VMkernel Binding with a vSphere Distributed Switch

You can configure VMkernel port binding for the RDMA adapter using a vSphere distributed switch and one uplink per switch. Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter.

1. Create a vSphere distributed switch with a VMkernel adapter and the network component.
   a) In the vSphere Client, select **Datacenter**, and click the **Networks** tab.
   b) Click **Actions** , and select **Distributed Switch** > **New Distributed Switch**.
   c) Select a name for the switch.
      Ensure that the location of the data center is present within your host, and click **Next**.
   d) Select the ESXi version as **7.0.0 and later**, and click **Next**.
   e) Enter the required number of uplinks, and click **Finish**.
2. Add one or more hosts to your distributed virtual switch.
   a) In the vSphere Client, select **Datacenter**, and click **Distributed Switches**..
      A list of available DSwitches appear.
   b) Right-click the DSwitch, and select **Add and Manage Hosts** from the menu.
   c) Select **Add hosts**, and click **Next**.
   d) Select your host, and click **Next**.
   e) Select **Assign uplink**.
   f) Enter the relevant uplink to assign the `vmnic`.
   g) Assign a VMkernel adapter, and click **Next**.
   h) In the vSphere Client, select the DSwitch, and click the **Ports** tab.
      You can view the uplinks created for your switch here.
3. Create distributed port groups for the NVMe over RDMA storage path.
   a) In the vSphere Client, select the required DSwitch.
   b) Click **Actions** and select **Distributed Port Group** > **New Distributed Port Group**.
   c) Under **Configure Settings**, enter the general properties of the port group.
      If you have configured a specific VLAN, add it in the VLAN ID.

      Note: Network connectivity issues might occur if you do not configure VLAN properly.

4. Configure the VMkernel adapters.
   a) In the vSphere Client, expand the **DSwitch** list, and select the distributed port group.
   b) Click **Actions** > **Add VMkernel Adapters**.
   c) In the **Select Member Hosts** dialog box, select your host and click **OK**.
   d) In the **Configure VMkernel Adapter** dialog box, ensure that the MTU matches to the Switch MTU.
   e) Under **Available services**, select **NVMe over RDMA** for appropriate tagging.
   f) Click **Finish**.
   g) Repeat step b and step c to add multiple RDMA capable NICs.
5. Set NIC teaming policies for the distributed port groups.
   a) In the **Distributed Port Group**, click **Actions** > **Edit Settings**.
   b) Click **Teaming and Failover**, and verify the active uplinks.
   c) Assign one uplink as **Active** for the port group, and the other uplink as **Unused**.
      Repeat step c for each of the port groups created.

After you complete the configuration, click **Configure**, and verify whether the physical adapter tab on your host lists the DVSwitch for the NICs selected.

Configure Adapters for NVMe over TCP Storage

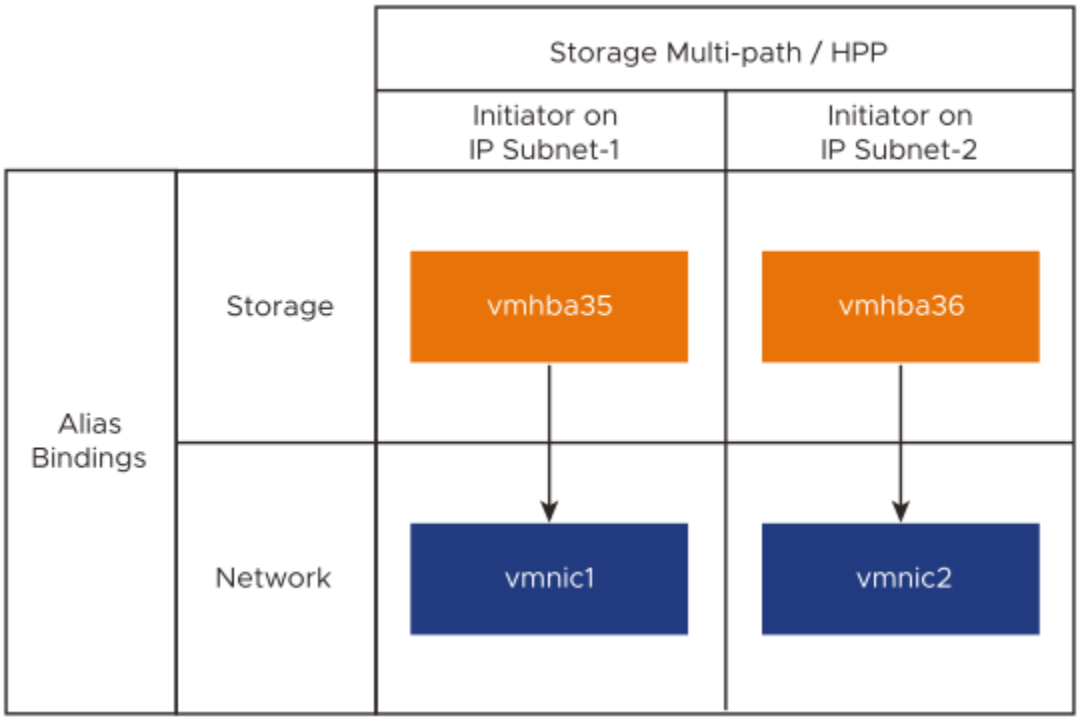
The adapter configuration process on the ESXi host involves setting up VMkernel binding for a TCP network adapter, and then enabling a software for NVMe over TCP adapter.

After you enable the software for NVMe over TCP adapter, add NVMe controllers so that the host can discover the NVMe targets. For more information, see Add Controller for NVMe over Fabrics.

Configure VMkernel Binding for the NVMe over TCP Adapter

Port binding for NVMe over TCP involves creating a virtual switch and connecting the physical network adapter and the VMkernel adapter to the virtual switch. Through this connection, the TCP adapter becomes bound to the VMkernel adapter. In the configuration, you can use a vSphere standard switch or a vSphere distributed switch.

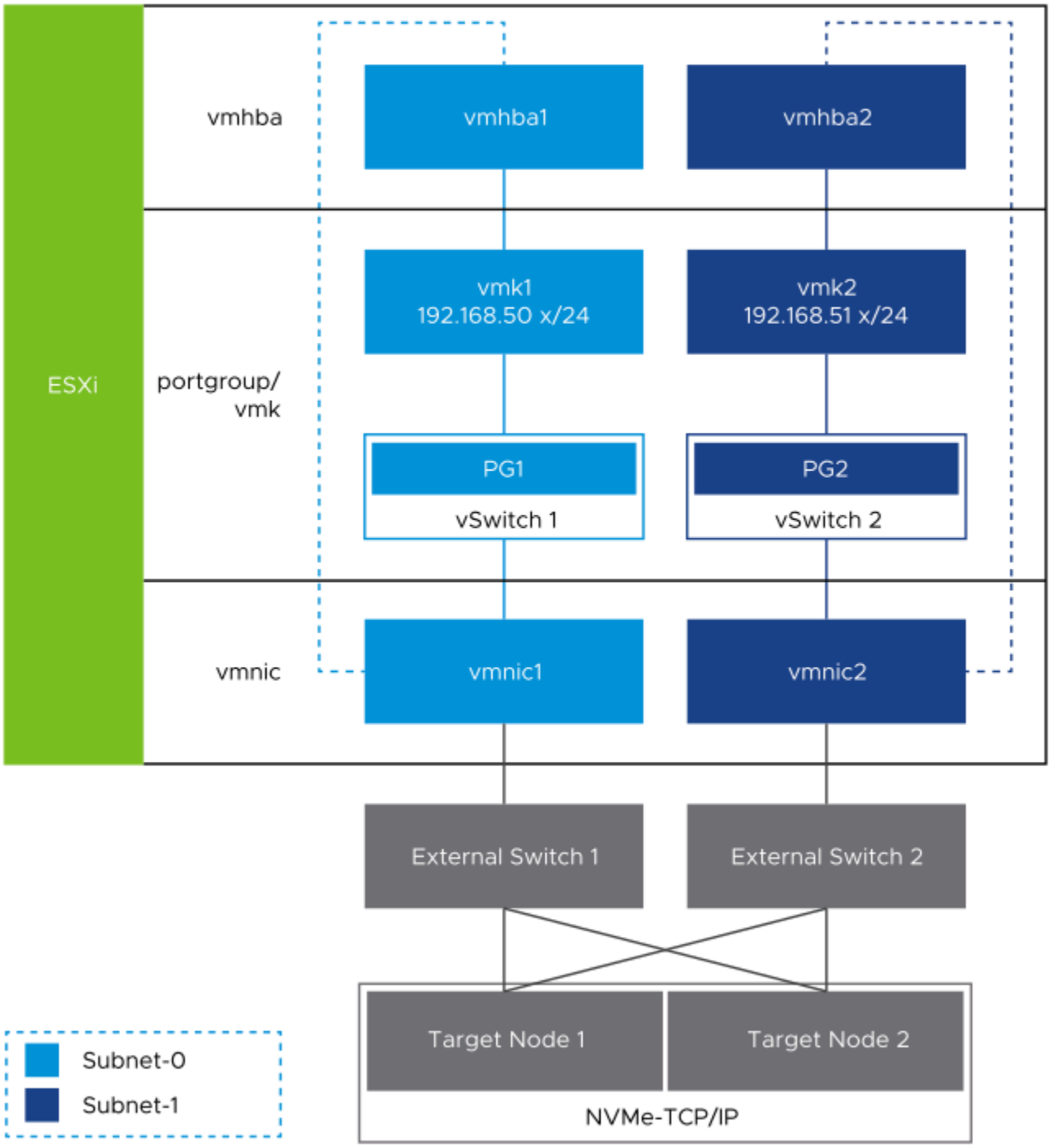
The following diagram displays the port binding for the NVMe over TCP adapter.



For more information about creating switches, see *Create a vSphere Standard Switch* or *Create a vSphere Distributed Switch* in the *vSphere Networking* documentation.

Example of Network Topology with NVMe over TCP

In this example, two vSphere standard switches and two network adapters (vmnic) on the host provide high availability. They connect to two external switches.


ESXi
vmhba
vmhba1
vmhba2
portgroup/
vmk
vmk1
192.168.50 x/24
vmk2
192.168.51 x/24
PG1
vSwitch 1
PG2
vSwitch 2
vmnic
vmnic1
vmnic2
External Switch 1
External Switch 2
Target Node 1
Target Node 2
NVMe-TCP/IP
Subnet-0
Subnet-1

Configure VMkernel Binding for the TCP Adapter with a vSphere Standard Switch

You can configure VMkernel port binding for the TCP adapter using a vSphere standard switch and one uplink per switch. Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter.

1. Create a vSphere standard switch with a VMkernel adapter and the network component.
   a) In the vSphere Client, select your host and click the **Networks** tab.
   b) Click **Actions** > **Add Networking**.
   c) Select **VMkernel Network Adapter** and click **NEXT**.
   d) Select **New standard switch** and click **NEXT**.
   e) Under **Assigned adapters**, click **+**.
      The list of available physical adapters is displayed.
   f) Select the required physical adapter `vmnic`, and click **OK**.

      Note: Make sure to select the physical network adapter that corresponds to the TCP/IP adapter.
   g) Under **VMkernel port settings**, enter the required values.
      If you are using VLAN for the storage path, enter the VLAN ID.
   h) In the **IP settings** list, enter the VMkernel IPv4 settings.
   i) Under **Available services**, select **NVMe over TCP** for appropriate tagging.
2. Verify that your switch is correctly configured.
   a) On the **Configure** tab, select **Virtual switches** under **Networking**.
   b) Expand the switch and verify its configuration.

      The illustration shows that the physical network adapter and the VMkernel adapter are connected to the vSphere standard switch. Through this connection, the TCP adapter is bound to the VMkernel adapter.

3. Set NIC teaming policies for vSphere standard switch.

   Note: The NVMe/TCP adapter does not support such NIC teaming features as failover and load balancing. Instead, it relies on Storage Multipathing for these functionalities. However, if you must configure NIC teaming for other network workloads on the uplink serving the NVMe/TCP adapter, follow these steps.

   a) Click the **Configure** tab, and select **Virtual switches** under **Networking**.
   b) Select the appropriate VMkernel adapter.
   c) From the right-click menu, click **Edit Settings**.
   d) Select **Teaming and Failover**.
   e) Under **Active adapters**, move the required physical adapter `vmnic`.
   f) Under **Standby adapters** > **Failover order**, move the other physcial adapters.
   g) Set appropriate load balancing and other properties.
   h) Repeat the steps to configure additional VMkernel adapters.

   To verify if the adapter is configured, click the **Configure** tab and select **VMkernel adapters**.

Configure VMkernel Binding for the TCP Adapter with a vSphere Distributed Switch

You can configure VMkernel port binding for the TCP adapter using a vSphere distributed switch and one uplink per switch. Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter.

1. Create a vSphere distributed switch with a VMkernel adapter and the network component.
   a) In the vSphere Client, select **Datacenter**, and click the **Networks** tab.
   b) Click **Actions** , and select **Distributed Switch** > **New Distributed Switch**.
   c) Select a name for the switch.

      Ensure that the location of the data center is present within your host, and click **Next**.
   d) Select the ESXi version as **ESXi 7.0 and later**, and click **Next**.
   e) Enter the required number of uplinks, and click **Finish**.
2. Add one or more hosts to your distributed virtual switch.
   a) In the vSphere Client, select **Datacenter**, and click **Distributed Switches**..

      A list of available DSwitches appear.
   b) Right-click the DSwitch, and select **Add and Manage Hosts** from the menu.
   c) Select **Add hosts**, and click **Next**.
   d) Select your host, and click **Next**.
   e) Select **Assign uplink**.
   f) Enter the relevant uplink to assign the `vmnic`.
   g) Assign a VMkernel adapter, and click **Next**.
   h) In the vSphere Client, select the DSwitch, and click the **Ports** tab.

      You can view the uplinks created for your switch here.
3. Create distributed port groups for the NVMe over TCP storage path.
   a) In the vSphere Client, select the required DSwitch.
   b) Click **Actions** and select **Distributed Port Group** > **New Distributed Port Group**.
   c) Under **Configure Settings**, enter the general properties of the port group.

      If you have configured a specific VLAN, add it in the VLAN ID.

      Note: Network connectivity issues might occur if you do not configure VLAN properly.

4. Configure the VMkernel adapters.
   a) In the vSphere Client, expand the **DSwitch** list, and select the distributed port group.
   b) Click **Actions** > **Add VMkernel Adapters**.
   c) In the **Select Member Hosts** dialog box, select your host and click **OK**.
   d) In the **Configure VMkernel Adapter** dialog box, ensure that the MTU matches to the Switch MTU.
   e) Click **Finish**.
   f) Repeat step b and step c to add multiple TCP capable NICs.
5. Set NIC teaming policies for the distributed port groups.

   Note: The NVMe/TCP adapter does not support such NIC teaming features as failover and load balancing. Instead, it relies on Storage Multipathing for these functionalities. However, if you must configure NIC teaming for other network workloads on the uplink serving the NVMe/TCP adapter, follow these steps.

   a) In the **Distributed Port Group**, click **Actions** > **Edit Settings**.
   b) Click **Teaming and Failover**, and verify the active uplinks.
   c) Assign one uplink as **Active** for the port group, and the other uplink as **Unused**.

      Repeat step c for each of the port groups created.

After you complete the configuration, click **Configure**, and verify whether the physical adapter tab on your host lists the DVSwitch for the NICs selected.

Enable NVMe over RDMA or NVMe over TCP Software Adapters

ESXi supports NVMe over RDMA and NVMe over TCP software adapters. Use the vSphere Client to enable the software storage adapters for NVMe over RDMA and NVMe over TCP.

- On your ESXi host, install an adapter that supports the following types of storage.
  - NVMe over RDMA adapter. For example, Mellanox Technologies MT27700 Family ConnectX-4.
  - NVMe over TCP adapter. For example, i40en.
- Configure the VMkernel binding for your adapters.
  - For NVMe over RDMA, see Configure VMkernel Binding for the RDMA Adapter.
  - For NVMe over TCP, see Configure VMkernel Binding for the NVMe over TCP Adapter.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and click the **Add Software Adapter** icon.
4. Select the adapter type as required.
   - **NVMe over RDMA adapter**
   - **NVMe over TCP adapter**
5. Depending on your selection in Step 4, select an appropriate RDMA adapter or TCP network adapter (`vmnic`) from the drop-down menu.

   Note: If you get an error message that prevents you from creating the software adapter, make sure that the VMkernel binding for the adapter is configured correctly. For more information, see Configure VMkernel Binding for the RDMA Adapter and Configure VMkernel Binding for the NVMe over TCP Adapter.

The software NVMe over RDMA and NVMe over TCP adapters appear in the list as `vmhba` storage adapters. You can remove the adapters if you need to free the underlying RDMA and TCP network adapter for other purposes.

Add Controller for NVMe over Fabrics

Use the vSphere Client to add an NVMe controller. After you add the controller, the NVMe namespaces associated with the controller become available to your ESXi host. The NVMe storage devices that represent the namespaces in the ESXi environment appear on the storage devices list.

Make sure that your ESXi host has appropriate adapters for your type of storage. See Requirements and Limitations of VMware NVMe Storage.

If you use NVMe over RDMA (RoCE v2) storage, you must add a controller after you configure a software NVMe over RDMA adapter. If you use NVMe over TCP storage, you must add a controller after you configure a software NVMe over TCP adapter. With FC-NVMe storage, after you install the required adapter, it automatically connects to all targets that are reachable at the moment. You can later reconfigure the adapter and disconnect its controllers or connect other controllers that were not available during the host boot.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter (vmhba#) to configure.
4. Click the **Controllers** tab, and click **Add Controller**.
5. To add the controller, select one of the following options, and click **Add**.

Option	Description
Automatically discover controllers	This method indicates that your host can accept a connection to any available controller. 1. Specify the following parameter for a discovery controller. – For NVMe over RDMA (RoCE v2), the IP address and transport port number. – For NVMe over TCP, the IP address, transport port number, and the digest parameter. 2. Click **Discover Controllers**. 3. From the list of controllers, select the controller to use.
Enter controller details manually	With this method, your host requests a connection to a specific controller with the following parameters: • Subsystem NQN • Target port identification. For NVMe over RDMA (RoCE v2), the IP address and transport port number (Optional). For FC-NVMe, the WorldWideNodeName and WorldWidePortName. • For NVMe over TCP, the IP address, transport port number (Optional), and the digest parameter (Optional). • Admin queue size. An optional parameter that specifies the size of the admin queue of the controller. A default value is 16. • Keepalive timeout. An optional parameter to specify in seconds the keep alive timeout between the adapter and the controller. A default timeout value is 60 seconds. • IO Queue Size and IO Queue Number. Optional parameters that can be set only through esxcli.

The controller appears on the list of controllers. Your host can now discover the NVMe namespaces that are associated with the controller. The NVMe storage devices that represent the namespaces in the ESXi environment appear on the storage devices list in the vSphere Client.

Remove NVMe over RDMA and TCP Software Adapters

Use the vSphere Client to remove NVMe over RDMA and TCP software adapters. You can remove the adapter if you need to free the underlying RDMA adapter or ethernet adapter for other purposes.

You cannot remove the NVMe over PCIe and FC-NVMe adapters.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Adapters**, and select the adapter (`vmhba#`) to remove.
4. Remove the NVMe controller connected to the adapter.
   a) Click the **Controllers** tab.
   b) Select the controller and click **Remove**.
      The NVMe controller is disconnected and disappears from the list.
5. Click the **Remove** icon (Remove the host's storage adapter) to remove the NVMe over RDMA adapter or the NVMe over TCP adapter.

Working with Datastores

Datastores are logical containers, analogous to file systems, that hide specifics of physical storage and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images.

Types of Datastores

Depending on the storage you use, datastores can be of different types.

vCenter Server and ESXi support the following types of datastores.

Table 213: Types of Datastores

Datastore Type	Description
VMFS (version 5 and 6)	Datastores that you deploy on block storage devices use the vSphere Virtual Machine File System (VMFS) format. VMFS is a special high-performance file system format that is optimized for storing virtual machines. See Understanding VMFS Datastores.
NFS (version 3 and 4.1)	An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume. The volume is located on a NAS server. The ESXi host mounts the volume as an NFS datastore, and uses it for storage needs. ESXi supports versions 3 and 4.1 of the NFS protocol. See Understanding Network File System Datastores
vSAN	vSAN aggregates all local capacity devices available on the hosts into a single datastore shared by all hosts in the vSAN cluster. See the *Administering VMware vSAN* documentation.
vVol	Virtual Volumes datastore represents a storage container in vCenter Server and vSphere Client. See Working with VMware vSphere Virtual Volumes.

Depending on your storage type, some of the following tasks are available for the datastores.

- Create datastores. You can use the vSphere Client to create certain types of datastores.
- Perform administrative operations on the datastores. Several operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.
- Organize the datastores. For example, you can group them into folders according to business practices. After you group the datastores, you can assign the same permissions and alarms on the datastores in the group at one time.
- Add the datastores to datastore clusters. A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create the datastore cluster, you can use Storage DRS to manage storage resources. For information about datastore clusters, see the *vSphere Resource Management* documentation.

Understanding VMFS Datastores

To store virtual disks, ESXi uses datastores. The datastores are logical containers that hide specifics of physical storage from virtual machines and provide a uniform model for storing the virtual machine files. The datastores that you deploy on block storage devices use the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing virtual machines.

Use the vSphere Client to set up the VMFS datastore in advance on the block-based storage device that your ESXi host discovers. The VMFS datastore can be extended to span over several physical storage devices that include SAN LUNs and local storage. This feature allows you to pool storage and gives you flexibility in creating the datastore necessary for your virtual machines.

You can increase the capacity of the datastore while the virtual machines are running on the datastore. This ability lets you add new space to your VMFS datastores as your virtual machine requires it. VMFS is designed for concurrent access from multiple physical machines and enforces the appropriate access controls on the virtual machine files.

Versions of VMFS Datastores

Several versions of the VMFS file system have been released since its introduction. Currently, ESXi supports VMFS5 and VMFS6.

For all supported VMFS version, ESXi offers complete read and write support. On the supported VMFS datastores, you can create and power on virtual machines.

Table 214: Host Access to VMFS Versions

VMFS	ESXi
VMFS6	Read and write
VMFS5	Read and write

The following table compares major characteristics of VMFS5 and VMFS6. For additional information, see *Configuration Maximums* .

Table 215: Comparing VMFS5 and VMFS6

Features and Functionalities	VMFS5	VMFS6
Access for ESXi hosts version 6.5 and later	Yes	Yes
Access for ESXi hosts version 6.0 and earlier	Yes	No
Datastores per host	512	512
512n storage devices	Yes	Yes (default)

Features and Functionalities	VMFS5	VMFS6
512e storage devices	Yes. Not supported on local 512e devices.	Yes (default)
4Kn storage devices	No	Yes
Automatic space reclamation	No	Yes
Manual space reclamation through the esxcli command. See Manually Reclaim Accumulated Storage Space.	Yes	Yes
Space reclamation from guest OS	Limited	Yes
GPT storage device partitioning	Yes	Yes
MBR storage device partitioning	Yes For a VMFS5 datastore that has been previously upgraded from VMFS3.	No
Storage devices greater than 2 TB for each VMFS extent	Yes	Yes
Support for virtual machines with large capacity virtual disks, or disks greater than 2 TB	Yes	Yes
Support of small files of 1 KB	Yes	Yes
Default use of ATS-only locking mechanisms on storage devices that support ATS. See VMFS Locking Mechanisms.	Yes	Yes
Block size	Standard 1 MB	Standard 1 MB
Default snapshots	VMFSsparse for virtual disks smaller than 2 TB. SEsparse for virtual disks larger than 2 TB.	SEsparse
Virtual disk emulation type	512n	512n
vMotion	Yes	Yes
Storage vMotion across different datastore types	Yes	Yes
High Availability and Fault Tolerance	Yes	Yes
DRS and Storage DRS	Yes	Yes
RDM	Yes	Yes

When you work with VMFS datastores, consider the following:

- Datastore Extents. A spanned VMFS datastore must use only homogeneous storage devices, either 512n, 512e, or 4Kn. The spanned datastore cannot extend over devices of different formats.
- Block Size. The block size on a VMFS datastore defines the maximum file size and the amount of space a file occupies. VMFS5 and VMFS6 datastores support the block size of 1 MB.
- Storage vMotion. Storage vMotion supports migration across VMFS, vSAN, and Virtual Volumes datastores. vCenter Server performs compatibility checks to validate Storage vMotion across different types of datastores.
- Storage DRS. VMFS5 and VMFS6 can coexist in the same datastore cluster. However, all datastores in the cluster must use homogeneous storage devices. Do not mix devices of different formats within the same datastore cluster.
- Device Partition Formats. Any new VMFS5 or VMFS6 datastore uses GUID partition table (GPT) to format the storage device. The GPT format enables you to create datastores larger than 2 TB. If your VMFS5 datastore has been previously upgraded from VMFS3, it continues to use the master boot record (MBR) partition format, which is characteristic for VMFS3. Conversion to GPT happens only after you expand the datastore to a size larger than 2 TB.

VMFS Datastores as Repositories

ESXi can format SCSI-based storage devices as VMFS datastores. VMFS datastores primarily serve as repositories for virtual machines.

Note: Always have only one VMFS datastore for each LUN.

You can store multiple virtual machines on the same VMFS datastore. Each virtual machine, encapsulated in a set of files, occupies a separate single directory. For the operating system inside the virtual machine, VMFS preserves the internal file system semantics, which ensures correct application behavior and data integrity for applications running in virtual machines.

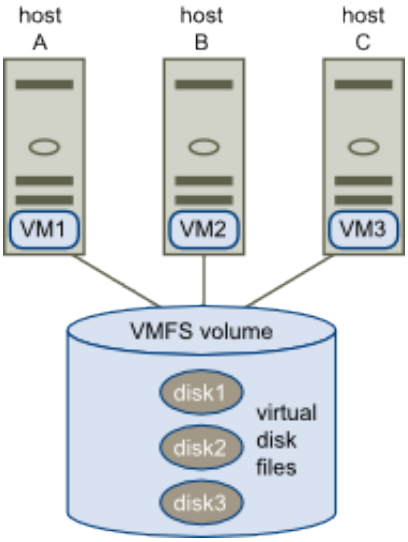
When you run multiple virtual machines, VMFS provides specific locking mechanisms for the virtual machine files. As a result, the virtual machines can operate safely in a SAN environment where multiple ESXi hosts share the same VMFS datastore.

In addition to the virtual machines, the VMFS datastores can store other files, such as the virtual machine templates and ISO images.

Sharing a VMFS Datastore Across Hosts

As a cluster file system, VMFS lets multiple ESXi hosts access the same VMFS datastore concurrently.

Figure 73: Sharing a VMFS Datastore Across Hosts



For information on the maximum number of hosts that can connect to a single VMFS datastore, see the *Configuration Maximums* document.

To ensure that multiple hosts do not access the same virtual machine at the same time, VMFS provides on-disk locking.

Sharing the VMFS volume across multiple hosts offers several advantages, for example, the following:

- You can use VMware Distributed Resource Scheduling (DRS) and VMware High Availability (HA).
  You can distribute virtual machines across different physical servers. That means you run a mix of virtual machines on each server, so that not all experience high demand in the same area at the same time. If a server fails, you can restart virtual machines on another physical server. If the failure occurs, the on-disk lock for each virtual machine is released. For more information about VMware DRS, see the *vSphere Resource Management* documentation. For information about VMware HA, see the *vSphere Availability* documentation.
- You can use vMotion to migrate running virtual machines from one physical server to another. For information about migrating virtual machines, see the *vCenter Server and Host Management* documentation.

To create a shared datastore, mount the datastore on those ESXi hosts that require the datastore access. See Mount Datastores.

VMFS Metadata Updates

A VMFS datastore holds virtual machine files, directories, symbolic links, RDM descriptor files, and so on. The datastore also maintains a consistent view of all the mapping information for these objects. This mapping information is called metadata.

Metadata is updated each time you perform datastore or virtual machine management operations. Examples of operations requiring metadata updates include the following:

- Creating, growing, or locking a virtual machine file
- Changing attributes of a file
- Powering a virtual machine on or off
- Creating or deleting a VMFS datastore
- Expanding a VMFS datastore
- Creating a template
- Deploying a virtual machine from a template
- Migrating a virtual machine with vMotion

When metadata changes are made in a shared storage environment, VMFS uses special locking mechanisms to protect its data and prevent multiple hosts from concurrently writing to the metadata.

VMFS Locking Mechanisms

In a shared storage environment, when multiple hosts access the same VMFS datastore, specific locking mechanisms are used. These locking mechanisms prevent multiple hosts from concurrently writing to the metadata and ensure that no data corruption occurs.

Depending on its configuration and the type of underlying storage, a VMFS datastore can use different types of locking mechanisms. It can exclusively use the atomic test and set locking mechanism (ATS-only), or use a combination of ATS and SCSI reservations (ATS+SCSI).

ATS-Only Mechanism

For storage devices that support T10 standard-based VAAI specifications, VMFS provides ATS locking, also called hardware assisted locking. The ATS algorithm supports discrete locking per disk sector. All newly formatted VMFS5 and VMFS6 datastores use the ATS-only mechanism if the underlying storage supports it, and never use SCSI reservations.

When you create a multi-extent datastore where ATS is used, vCenter Server filters out non-ATS devices. This filtering allows you to use only those devices that support the ATS primitive.

In certain cases, you might need to change the default locking mechanism for a VMFS5 or VMFS6 datastore. For information, see Change Locking Mechanism to ATS+SCSI.

Note: If you are running a VMware vSAN environment or have ATS-only VMFS volumes, do not deactivate ATS. Deactivating ATS might result in an outage as no locking mechanism is available. For more information, see a VMware Knowledge Base article.

ATS+SCSI Mechanism

A VMFS datastore that supports the ATS+SCSI mechanism is configured to use ATS and attempts to use it when possible. If ATS fails, the VMFS datastore reverts to SCSI reservations. In contrast with the ATS locking, the SCSI

reservations lock an entire storage device while an operation that requires metadata protection is performed. After the operation completes, VMFS releases the reservation, and other operations can continue.

Datastores that use the ATS+SCSI mechanism include VMFS5 datastores that were upgraded from VMFS3. In addition, new VMFS5 or VMFS6 datastores on storage devices that do not support ATS use the ATS+SCSI mechanism.

If the VMFS datastore reverts to SCSI reservations, you might notice performance degradation caused by excessive SCSI reservations.

Display VMFS Locking Information

Use the `esxcli` command to obtain information about the locking mechanism that a VMFS datastore uses.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To display information related to VMFS locking mechanisms, run the following command:

```
esxcli storage vmfs lockmode list
```

The table lists items that the output of the command might include.

Table 216: VMFS Locking Information

Fields	Values	Descriptions
Locking Modes		Indicates the locking configuration of the datastore.
	`ATS`	The datastore is configured to use the ATS-only locking mode.
	`ATS+SCSI`	The datastore is configured to use the ATS mode. If ATS fails or is not supported, the datastore can revert to SCSI.
	`ATS upgrade pending`	The datastore is in the process of an online upgrade to the ATS-only mode.
	`ATS downgrade pending`	The datastore is in the process of an online downgrade to the ATS+SCSI mode.
ATS Compatible		Indicates whether the datastore can be or cannot be configured for the ATS-only mode.
ATS Upgrade Modes		Indicates the type of upgrade that the datastore supports.
	`None`	The datastore is not ATS-only compatible.
	`Online`	The datastore can be used during its upgrade to the ATS-only mode.
	`Offline`	The datastore cannot be used during its upgrade to the ATS-only mode.
ATS Incompatibility Reason		If the datastore is not compatible with ATS-only, the item indicates the reason for the incompatibility.

Change VMFS Locking to ATS-Only

If your VMFS datastore uses the ATS+SCSI locking mechanism, you can change to ATS-only locking.

Typically, VMFS5 datastores that were previously upgraded from VMFS3 continue using the ATS+SCSI locking mechanism. If the datastores are deployed on ATS-enabled hardware, they are eligible for an upgrade to ATS-only locking. Depending on your vSphere environment, you can use one of the following upgrade modes:

- The online upgrade to the ATS-only mechanism is available for most single-extent VMFS5 datastores. While you perform the online upgrade on one of the hosts, other hosts can continue using the datastore.
- The offline upgrade to ATS-only must be used for VMFS5 datastores that span multiple physical extents. Datastores composed of multiple extents are not eligible for the online upgrade. These datastores require that no hosts actively use the datastores at the time of the upgrade request.

Prepare for an Upgrade to ATS-Only Locking

You must perform several steps to prepare your environment for an online or offline upgrade to ATS-only locking.

1. Upgrade all hosts that access the VMFS5 datastore to the newest version of vSphere.
2. Determine whether the datastore is eligible for an upgrade of its current locking mechanism by running the `esxcli storage vmfs lockmode list` command.

   The following sample output indicates that the datastore is eligible for an upgrade. It also shows the current locking mechanism and the upgrade mode available for the datastore.

   ```
   Locking Mode  ATS Compatible  ATS Upgrade Modes
   ------------  --------------  -----------------
   ATS+SCSI           true       Online or Offline
   ```

3. Depending on the upgrade mode available for the datastore, perform one of the following actions:

Upgrade Mode	Action
Online	Verify that all hosts have consistent storage connectivity to the VMFS datastore.
Offline	Verify that no hosts are actively using the datastore.

Upgrade Locking Mechanism to the ATS-Only Type

If a VMFS datastore is ATS-only compatible, you can upgrade its locking mechanism from ATS+SCSI to ATS-only.

If you plan to complete the upgrade of the locking mechanism by putting the datastore into maintenance mode, disable Storage DRS. This prerequisite applies only to an online upgrade.

Most datastores that do not span multiple extents are eligible for an online upgrade. While you perform the online upgrade on one of the ESXi hosts, other hosts can continue using the datastore. The online upgrade completes only after all hosts have closed the datastore.

1. Perform an upgrade of the locking mechanism by running the following command:

   `esxcli storage vmfs lockmode set -a|--ats -l|--volume-label=`*`VMFS label`* `-u|--volume-uuid=`*`VMFS UUID`*.

2. For an online upgrade, perform additional steps.
   a) Close the datastore on all hosts that have access to the datastore, so that the hosts can recognize the change.

      You can use one of the following methods:

      - Unmount and mount the datastore.

- Put the datastore into maintenance mode and exit maintenance mode.

b) Verify that the Locking Mode status for the datastore changed to ATS-only by running:

```
esxcli storage vmfs lockmode list
```

c) If the Locking Mode displays any other status, for example ATS UPGRADE PENDING, check which host has not yet processed the upgrade by running:

```
esxcli storage vmfs host list
```

Change Locking Mechanism to ATS+SCSI

When you create a VMFS5 datastore on a device that supports the atomic test and set (ATS) locking, the datastore uses the ATS-only locking mechanism. In certain circumstances, you might need to downgrade the ATS-only locking to ATS +SCSI.

You might need to switch to the ATS+SCSI locking mechanism when, for example, your storage device is downgraded. Or when firmware updates fail and the device no longer supports ATS.
The downgrade process is similar to the ATS-only upgrade. As with the upgrade, depending on your storage configuration, you can perform the downgrade in online or offline mode.

Note: If you are running a VMware vSAN environment or have ATS-only VMFS volumes, do not deactivate ATS. Deactivating ATS might result in an outage as no locking mechanism is available. For more information, see a VMware Knowledge Base article.

1. Change the locking mechanism to ATS+SCSI by running the following command:

   `esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label=` *`VMFS label`* `-u|--volume-uuid=` *`VMFS UUID`*.

2. For an online mode, close the datastore on all hosts that have access to the datastore, so that the hosts can recognize the change.

Snapshot Formats on VMFS

When you take a snapshot, the state of the virtual disk is preserved, which prevents the guest operating system from writing to it. A delta or child disk is created. The delta represents the difference between the current state of the VM disk and the state that existed when you took the previous snapshot. On the VMFS datastore, the delta disk is a sparse disk.

Sparse disks use the copy-on-write mechanism, in which the virtual disk contains no data, until the data is copied there by a write operation. This optimization saves storage space.

Depending on the type of your datastore, delta disks use different sparse formats.

Snapshot Formats	VMFS5	VMFS6
VMFSsparse	For virtual disks smaller than 2 TB.	N/A
SEsparse	For virtual disks larger than 2 TB.	For all disks.

VMFSsparse

VMFS5 uses the VMFSsparse format for virtual disks smaller than 2 TB.

VMFSsparse is implemented on top of VMFS. The VMFSsparse layer processes I/Os issued to a snapshot VM. Technically, VMFSsparse is a redo-log that starts empty, immediately after a VM snapshot is taken. The redo-log expands to the size of its base vmdk, when the entire vmdk is rewritten with new data after the VM snapshotting. This redo-log is a file in the VMFS datastore. Upon snapshot creation, the base vmdk attached to the VM is changed to the newly created sparse vmdk.

SEsparse	SEsparse is a default format for all delta disks on the VMFS6 datastores. On VMFS5, SEsparse is used for virtual disks of the size 2 TB and larger. SEsparse is a format similar to VMFSsparse with some enhancements. This format is space efficient and supports the space reclamation technique. With space reclamation, blocks that the guest OS deletes are marked. The system sends commands to the SEsparse layer in the hypervisor to unmap those blocks. The unmapping helps to reclaim space allocated by SEsparse once the guest operating system has deleted that data. For more information about space reclamation, see Storage Space Reclamation.

Snapshot Migration

You can migrate VMs with snapshots across different datastores. The following considerations apply:

- If you migrate a VM with the VMFSsparse snapshot to VMFS6, the snapshot format changes to SEsparse.
- When a VM with a vmdk of the size smaller than 2 TB is migrated to VMFS5, the snapshot format changes to VMFSsparse.
- You cannot mix VMFSsparse redo-logs with SEsparse redo-logs in the same hierarchy.

Upgrading VMFS Datastores

ESXi uses different approaches to VMFS5 and VMFS3 upgrades.

VMFS5 Datastores

You cannot upgrade a VMFS5 datastore to VMFS6. If you have a VMFS5 datastore in your environment, create a VMFS6 datastore and migrate virtual machines from the VMFS5 datastore to VMFS6.

VMFS3 Datastores

ESXi no longer supports VMFS3 datastores. The ESXi host automatically upgrades VMFS3 to VMFS5 when mounting existing datastores. The host performs the upgrade operation in the following circumstances:

- At the first boot after an upgrade to ESXi 7.0 or later, when the host mounts all discovered VMFS3 datastores.
- When you manually mount the VMFS3 datastores that are discovered after the boot, or mount persistently unmounted datastores.

Understanding Network File System Datastores

An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume that is located on a NAS server. The ESXi host can mount the volume and use it for its storage needs. vSphere supports versions 3 and 4.1 of the NFS protocol.

Typically, the NFS volume or directory is created by a storage administrator and is exported from the NFS server. You do not need to format the NFS volume with a local file system, such as VMFS. Instead, you mount the volume directly on the ESXi hosts and use it to store and boot virtual machines in the same way that you use the VMFS datastores.

In addition to storing virtual disks on NFS datastores, you can use NFS as a central repository for ISO images, virtual machine templates, and so on. If you use the datastore for the ISO images, you can connect the CD-ROM device of the virtual machine to an ISO file on the datastore. You then can install a guest operating system from the ISO file.

NFS Protocols and ESXi

ESXi supports NFS protocols version 3 and 4.1. To support both versions, ESXi uses two different NFS clients.

Comparing Versions of NFS Clients

The following table lists capabilities that the NFS version 3 and 4.1 support.

Characteristics	NFS version 3	NFS version 4.1
Security mechanisms	AUTH_SYS	AUTH_SYS and Kerberos (krb5 and krb5i)
Encryption algorithms with Kerberos	N/A	AES256-CTS-HMAC-SHA1-96 and AES128-CTS-HMAC-SHA1-96
Multipathing	Not supported	Supported through the session trunking
Locking mechanisms	Propriety client-side locking	Server-side locking
Hardware acceleration	Supported	Supported
Thick virtual disks	Supported	Supported
IPv6	Supported	Supported for AUTH_SYS and Kerberos
ISO images presented as CD-ROMs to virtual machines	Supported	Supported
Virtual machine snapshots	Supported	Supported
Virtual machines with virtual disks greater than 2 TB	Supported	Supported

NFS Protocols and vSphere Solutions

The following table lists major vSphere solutions that NFS versions support.

vSphere Features	NFS version 3	NFS version 4.1
vMotion and Storage vMotion	Yes	Yes
High Availability (HA)	Yes	Yes
Fault Tolerance (FT)	Yes	Yes
Distributed Resource Scheduler (DRS)	Yes	Yes
Host Profiles	Yes	Yes
Storage DRS	Yes	No
Storage I/O Control	Yes	No
Site Recovery Manager	Yes	Site Recovery Manager does not support NFS 4.1 datastores for array-based replication and Virtual Volumes replication. You can use Site Recovery Manager with NFS v 4.1 datastores for vSphere Replication.
Virtual Volumes	Yes	Yes
vSphere Replication	Yes	Yes
vRealize Operations Manager	Yes	Yes

NFS 4.1 and Fault Tolerance

Virtual machines on NFS 4.1 support the new Fault Tolerance mechanism that was introduced in vSphere 6.0. The mechanism can accommodate symmetric multiprocessor (SMP) virtual machines with up to four vCPUs.

NFS 4.1 VMs do not support the legacy Fault Tolerance mechanism.

NFS Upgrades

When you upgrade ESXi from a version earlier than 6.5, existing NFS 4.1 datastores automatically begin supporting functionalities that were not available in the previous ESXi release. These functionalities include Virtual Volumes, hardware acceleration, and so on.

ESXi does not support automatic datastore conversions from NFS version 3 to NFS 4.1.

If you want to upgrade your NFS 3 datastore, the following options are available:

- Create the NFS 4.1 datastore, and then use Storage vMotion to migrate virtual machines from the old datastore to the new one.
- Use conversion methods provided by your NFS storage server. For more information, contact your storage vendor.
- Unmount the NFS 3 datastore, and then mount as NFS 4.1 datastore.
  CAUTION: If you use this option, make sure to unmount the datastore from all hosts that have access to the datastore. The datastore can never be mounted by using both protocols at the same time.

NFS Storage Guidelines and Requirements

When you use NFS storage, follow specific guidelines related to NFS server configuration, networking, NFS datastores, and so on.

NFS Server Configuration

When you configure NFS servers to work with ESXi, follow recommendation of your storage vendor. In addition to these general recommendations, use specific guidelines that apply to NFS in vSphere environment.

The guidelines include the following items.

- Make sure that the NAS servers you use are listed in the *VMware HCL*. Use the correct version for the server firmware.
- Ensure that the NFS volume is exported using NFS over TCP.
- Make sure that the NAS server exports a particular share as either NFS 3 or NFS 4.1. The NAS server must not provide both protocol versions for the same share. The NAS server must enforce this policy because ESXi does not prevent mounting the same share through different NFS versions.
- NFS 3 and non-Kerberos (AUTH_SYS) NFS 4.1 do not support the delegate user functionality that enables access to NFS volumes using nonroot credentials. If you use NFS 3 or non-Kerberos NFS 4.1, ensure that each host has root access to the volume. Different storage vendors have different methods of enabling this functionality, but typically the NAS servers use the `no_root_squash` option. If the NAS server does not grant root access, you can still mount the NFS datastore on the host. However, you cannot create any virtual machines on the datastore.
- If the underlying NFS volume is read-only, make sure that the volume is exported as a read-only share by the NFS server. Or mount the volume as a read-only datastore on the ESXi host. Otherwise, the host considers the datastore to be read-write and might not open the files.

NFS Networking

An ESXi host uses TCP/IP network connection to access a remote NAS server. Certain guidelines and best practices exist for configuring the networking when you use NFS storage.

For more information, see the *vSphere Networking* documentation.

- For network connectivity, use a standard network adapter in your ESXi host.
- ESXi supports Layer 2 and Layer 3 Network switches. If you use Layer 3 switches, ESXi hosts and NFS storage arrays must be on different subnets and the network switch must handle the routing information.
- Configure a VMkernel port group for NFS storage. You can create the VMkernel port group for IP storage on an existing virtual switch (vSwitch) or on a new vSwitch. The vSwitch can be a vSphere Standard Switch (VSS) or a vSphere Distributed Switch (VDS).
- If you use multiple ports for NFS traffic, make sure that you correctly configure your virtual switches and physical switches.
- NFS 3 and NFS 4.1 support IPv6.

NFS File Locking

File locking mechanisms are used to restrict access to data stored on a server to only one user or process at a time. The locking mechanisms of the two NFS versions are not compatible. NFS 3 uses proprietary locking and NFS 4.1 uses native protocol specified locking.

NFS 3 locking on ESXi does not use the Network Lock Manager (NLM) protocol. Instead, VMware provides its own locking protocol. NFS 3 locks are implemented by creating lock files on the NFS server. Lock files are named `.lck-`*`file_id`*`..`

NFS 4.1 uses share reservations as a locking mechanism.

Because NFS 3 and NFS 4.1 clients do not use the same locking protocol, you cannot use different NFS versions to mount the same datastore on multiple hosts. Accessing the same virtual disks from two incompatible clients might result in incorrect behavior and cause data corruption.

NFS Security

With NFS 3 and NFS 4.1, ESXi supports the AUTH_SYS security. In addition, for NFS 4.1, the Kerberos security mechanism is supported.

NFS 3 supports the AUTH_SYS security mechanism. With this mechanism, storage traffic is transmitted in an unencrypted format across the LAN. Because of this limited security, use NFS storage on trusted networks only and isolate the traffic on separate physical switches. You can also use a private VLAN.

NFS 4.1 supports the Kerberos authentication protocol to secure communications with the NFS server. Nonroot users can access files when Kerberos is used. For more information, see Using Kerberos for NFS 4.1.

In addition to Kerberos, NFS 4.1 supports traditional non-Kerberos mounts with the AUTH_SYS security. In this case, use root access guidelines for NFS version 3.

Note: You cannot use two security mechanisms, AUTH_SYS and Kerberos, for the same NFS 4.1 datastore shared by multiple hosts.

NFS Multipathing

NFS 4.1 supports multipathing as per protocol specifications. For NFS 3 multipathing is not applicable.

NFS 3 uses one TCP connection for I/O. As a result, ESXi supports I/O on only one IP address or hostname for the NFS server, and does not support multiple paths. Depending on your network infrastructure and configuration, you can use the network stack to configure multiple connections to the storage targets. In this case, you must have multiple datastores, each datastore using separate network connections between the host and the storage.

NFS 4.1 provides multipathing for servers that support the session trunking. When the trunking is available, you can use multiple IP addresses to access a single NFS volume. Client ID trunking is not supported.

NFS and Hardware Acceleration

Virtual disks created on NFS datastores are thin-provisioned by default. To be able to create thick-provisioned virtual disks, you must use hardware acceleration that supports the Reserve Space operation.

NFS 3 and NFS 4.1 support hardware acceleration that allows your host to integrate with NAS devices and use several hardware operations that NAS storage provides. For more information, see Hardware Acceleration on NAS Devices.

NFS Datastores

When you create an NFS datastore, make sure to follow specific guidelines.

The NFS datastore guidelines and best practices include the following items:

- You cannot use different NFS versions to mount the same datastore on different hosts. NFS 3 and NFS 4.1 clients are not compatible and do not use the same locking protocol. As a result, accessing the same virtual disks from two incompatible clients might result in incorrect behavior and cause data corruption.
- NFS 3 and NFS 4.1 datastores can coexist on the same host.
- ESXi cannot automatically upgrade NFS version 3 to version 4.1, but you can use other conversion methods. For information, see NFS Protocols and ESXi.
- When you mount the same NFS 3 volume on different hosts, make sure that the server and folder names are identical across the hosts. If the names do not match, the hosts see the same NFS version 3 volume as two different datastores. This error might result in a failure of such features as vMotion. An example of such discrepancy is entering `filer` as the server name on one host and `filer.domain.com` on the other. This guideline does not apply to NFS version 4.1.
- If you use non-ASCII characters to name datastores and virtual machines, make sure that the underlying NFS server offers internationalization support. If the server does not support international characters, use only ASCII characters, or unpredictable failures might occur.

Firewall Configurations for NFS Storage

ESXi includes a firewall between the management interface and the network. The firewall is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for the default services, such as NFS.

Supported services, including NFS, are described in a rule set configuration file in the ESXi firewall directory `/etc/vmware/firewall/`. The file contains firewall rules and their relationships with ports and protocols.

The behavior of the NFS Client rule set (`nfsClient`) is different from other rule sets.

For more information about firewall configurations, see the *vSphere Security* documentation.

NFS Client Firewall Behavior

The NFS Client firewall rule set behaves differently than other ESXi firewall rule sets. ESXi configures NFS Client settings when you mount or unmount an NFS datastore. The behavior differs for different versions of NFS.

When you add, mount, or unmount an NFS datastore, the resulting behavior depends on the version of NFS.

NFS v3 Firewall Behavior

When you add or mount an NFS v3 datastore, ESXi checks the state of the NFS Client (`nfsClient`) firewall rule set.

- If the `nfsClient` rule set is disabled, ESXi enables the rule set and disables the Allow All IP Addresses policy by setting the `allowedAll` flag to `FALSE`. The IP address of the NFS server is added to the allowed list of outgoing IP addresses.
- If the `nfsClient` rule set is enabled, the state of the rule set and the allowed IP address policy are not changed. The IP address of the NFS server is added to the allowed list of outgoing IP addresses.

Note: If you manually enable the `nfsClient` rule set or manually set the Allow All IP Addresses policy, either before or after you add an NFS v3 datastore to the system, your settings are overridden when the last NFS v3 datastore is unmounted. The `nfsClient` rule set is disabled when all NFS v3 datastores are unmounted.

When you remove or unmount an NFS v3 datastore, ESXi performs one of the following actions.

- If none of the remaining NFS v3 datastores are mounted from the server of the datastore being unmounted, ESXi removes the server's IP address from the list of outgoing IP addresses.
- If no mounted NFS v3 datastores remain after the unmount operation, ESXi disables the `nfsClient` firewall rule set.

NFS v4.1 Firewall Behavior

When you mount the first NFS v4.1 datastore, ESXi enables the `nfs41client` rule set and sets its `allowedAll` flag to TRUE. This action opens port 2049 for all IP addresses. Unmounting an NFS v4.1 datastore does not affect the firewall state. That is, the first NFS v4.1 mount opens port 2049 and that port remains enabled unless you close it explicitly.

Verify Firewall Ports for NFS Clients

To enable access to NFS storage, ESXi automatically opens firewall ports for the NFS clients when you mount an NFS datastore. For troubleshooting reasons, you might need to verify that the ports are open.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Firewall**, and click **Edit**.
4. Scroll down to an appropriate version of NFS to make sure that the port is open.

Using Layer 3 Routed Connections to Access NFS Storage

When you use Layer 3 (L3) routed connections to access NFS storage, consider certain requirements and restrictions.

Ensure that your environment meets the following requirements:

- Use Cisco's Hot Standby Router Protocol (HSRP) in IP Router. If you are using a non-Cisco router, use Virtual Router Redundancy Protocol (VRRP) instead.
- To prioritize NFS L3 traffic on networks with limited bandwidths, or on networks that experience congestion, use Quality of Service (QoS). See your router documentation for details.
- Follow Routed NFS L3 recommendations offered by storage vendor. Contact your storage vendor for details.
- Disable Network I/O Resource Management (NetIORM).
- If you are planning to use systems with top-of-rack switches or switch-dependent I/O device partitioning, contact your system vendor for compatibility and support.

In an L3 environment, the following restrictions apply:

- The environment does not support VMware Site Recovery Manager.

- The environment supports only the NFS protocol. Do not use other storage protocols such as FCoE over the same physical network.
- The NFS traffic in this environment does not support IPv6.
- The NFS traffic in this environment can be routed only over a LAN. Other environments such as WAN are not supported.

Using Kerberos for NFS 4.1

With NFS version 4.1, ESXi supports the Kerberos authentication mechanism.

The RPCSEC_GSS Kerberos mechanism is an authentication service. It allows an NFS 4.1 client installed on ESXi to prove its identity to an NFS server before mounting an NFS share. The Kerberos security uses cryptography to work across an insecure network connection.

The ESXi implementation of Kerberos for NFS 4.1 provides two security models, krb5 and krb5i, that offer different levels of security.

- Kerberos for authentication only (krb5) supports identity verification.
- Kerberos for authentication and data integrity (krb5i), in addition to identity verification, provides data integrity services. These services help to protect the NFS traffic from tampering by checking data packets for any potential modifications.

Kerberos supports cryptographic algorithms that prevent unauthorized users from gaining access to NFS traffic. The NFS 4.1 client on ESXi attempts to use either the AES256-CTS-HMAC-SHA1-96 or AES128-CTS-HMAC-SHA1-96 algorithm to access a share on the NAS server. Before using your NFS 4.1 datastores, make sure that AES256-CTS-HMAC-SHA1-96 or AES128-CTS-HMAC-SHA1-96 are enabled on the NAS server.

The following table compares Kerberos security levels that ESXi supports.

Table 217: Types of Kerberos Security

		ESXi 6.0	ESXi 6.5 and later
Kerberos for authentication only (krb5)	Integrity checksum for RPC header	Yes with DES	Yes with AES
	Integrity checksum for RPC data	No	No
Kerberos for authentication and data integrity (krb5i)	Integrity checksum for RPC header	No krb5i	Yes with AES
	Integrity checksum for RPC data		Yes with AES

When you use Kerberos authentication, the following considerations apply:

- ESXi uses Kerberos with the Active Directory domain.
- As a vSphere administrator, you specify Active Directory credentials to provide access to NFS 4.1 Kerberos datastores for an NFS user. A single set of credentials is used to access all Kerberos datastores mounted on that host.
- When multiple ESXi hosts share the NFS 4.1 datastore, you must use the same Active Directory credentials for all hosts that access the shared datastore. To automate the assignment process, set the user in host profiles and apply the profile to all ESXi hosts.
- You cannot use two security mechanisms, AUTH_SYS and Kerberos, for the same NFS 4.1 datastore shared by multiple hosts.

Set Up NFS Storage Environment

You must perform several configuration steps before you mount an NFS datastore in vSphere.

- Familiarize yourself with the guidelines in NFS Storage Guidelines and Requirements.
- For details on configuring NFS storage, consult your storage vendor documentation.
- If you use Kerberos, make sure that AES256-CTS-HMAC-SHA1-96 or AES128-CTS-HMAC-SHA1-96 are enabled on the NAS server.

1. On the NFS server, configure an NFS volume and export it to be mounted on the ESXi hosts.
   a) Note the IP address or the DNS name of the NFS server and the full path, or folder name, for the NFS share.
      For NFS 4.1, you can collect multiple IP addresses or DNS names to use the multipathing support that the NFS 4.1 datastore provides.
   b) If you plan to use Kerberos authentication with NFS 4.1, specify the Kerberos credentials to be used by ESXi for authentication.
2. On each ESXi host, configure a VMkernel Network port for NFS traffic.
   For more information, see the *vSphere Networking* documentation.
3. If you plan to use Kerberos authentication with the NFS 4.1 datastore, configure the ESXi hosts for Kerberos authentication.
   See Configure ESXi Hosts for Kerberos Authentication.

You can now create an NFS datastore on the ESXi hosts.

Configure ESXi Hosts for Kerberos Authentication

If you use NFS 4.1 with Kerberos, you must perform several tasks to set up your hosts for Kerberos authentication.

- Make sure that Microsoft Active Directory (AD) and NFS servers are configured to use Kerberos.
- Enable AES256-CTS-HMAC-SHA1-96 or AES128-CTS-HMAC-SHA1-96 encryption modes on AD. The NFS 4.1 client does not support the DES-CBC-MD5 encryption mode.
- Make sure that the NFS server exports are configured to grant full access to the Kerberos user.

When multiple ESXi hosts share the NFS 4.1 datastore, you must use the same Active Directory credentials for all hosts that access the shared datastore. You can automate the assignment process by setting the user in host profiles and applying the profile to all ESXi hosts.

After you configure your host for Kerberos, you can create an NFS 4.1 datastore with Kerberos enabled.

Configure DNS for NFS 4.1 with Kerberos

When you use NFS 4.1 with Kerberos, you must change the DNS settings on ESXi hosts. The settings must point to the DNS server that is configured to hand out DNS records for the Kerberos Key Distribution Center (KDC). For example, use the Active Directory server address if AD is used as a DNS server.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Networking**, click **TCP/IP configuration**.
4. Select **Default** and click the **Edit** icon.
5. Manually enter the DNS settings.

Option	Description
Domain	*AD Domain Name*
Preferred DNS server	*AD Server IP*
Search domains	*AD Domain Name*

Configure Network Time Protocol for NFS 4.1 with Kerberos

If you use NFS 4.1 with Kerberos, ESXi hosts, the NFS server, and the Active Domain server need to be time synchronized. Typically, in the setup the Active Domain server is used as the Network Time Protocol (NTP) server.

The following task describes how to synchronize the ESXi host with the NTP server.

The best practice is to use the Active Domain server as the NTP server.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, select **Time Configuration**.
4. Click **Edit** and set up the NTP server.
   a) Select **Use Network Time Protocol (Enable NTP client)**.
   b) To synchronize with the NTP server, enter its IP addresses.
   c) Select **Start NTP Service**.
   d) Set the NTP Service Startup Policy.
5. Click **OK**.
   The host synchronizes with the NTP server.

Enable Kerberos Authentication in Active Directory

If you use NFS 4.1 storage with Kerberos, you must add each ESXi host to an Active Directory domain and enable Kerberos authentication. Kerberos integrates with Active Directory to enable single sign-on and provides an extra layer of security when used across an insecure network connection.

Set up an AD domain and a domain administrator account with the rights to add hosts to the domain.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Authentication Services**.
4. Add the ESXi host to an Active Directory domain.
   a) In the Authentication Services pane, click **Join Domain**.
   b) Supply the domain settings, and click **OK**.
   The directory services type changes to Active Directory.
5. Configure or edit credentials for an NFS Kerberos user.
   a) In the NFS Kerberos Credentials pane, click **Edit**.
   b) Enter a user name and password.
      Files stored in all Kerberos datastores are accessed using these credentials.
   The state for NFS Kerberos credentials changes to Enabled.

Collecting Statistical Information for NFS Storage

You can use the `nfsStats` tool in your ESXi host to display statistical information about NFS calls and Remote Procedure Calls (RPC). The command displays statistical information for NFS 3 and NFS 4.1 mounts on the ESXi host.

Generally, the `nfsStats` tool performs the following tasks.

- Gathers NFS statistics to investigate problems when you deploy a new configuration, such as a new NFS server or network, in the NFS environment.

- Provides statistics about the success and failure of NFS operations.
- Publishes latency statistics about the success and failure of NFS operations.
- Troubleshoots NFS performance issues.

The command syntax is `nfsStats`*`options`*.

The following command options are available.

Table 218: nfsStats commands

Command Option	Description
No option	Obtain both NFS statistics and RPC statistics for all NFS datastores.
-3	Display only NFS 3 statistics.
-4	Display only NFS 4.1 statistics.
-n	Display only NFS 3 and NFS 4.1 statistics.
-r	Display RPC statistics.
-i*interval*	Display NFS and RPC statistics at an interval equal to the specified value in seconds. For example, if the value you enter is 10, the statistics is refreshed every 10 seconds.
-v*DSNAME1, DSNAME2, ...*	Display both NFS and RPC statistics for the specified NFS datastores. Use this option in conjunction with the type of the NFS datastore, for example, -3 or -4.
-j	Display statistics in json format.

Creating Datastores

You use the New Datastore wizard to create your datastores. Depending on the type of your storage and storage needs, you can create a VMFS, NFS, or Virtual Volumes datastore.

A vSAN datastore is automatically created when you enable vSAN. For information, see the *Administering VMware vSAN* documentation.

You can also use the New Datastore wizard to manage VMFS datastore copies.

Create a VMFS Datastore

VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that the host discovers, including Fibre Channel, iSCSI, and local storage devices.

1. Install and configure any adapters that your storage requires.
2. To discover newly added storage devices, perform a rescan. See Storage Rescan Operations.
3. Verify that storage devices you are planning to use for your datastores are available. See Storage Device Characteristics.

1. In the vSphere Client object navigator, browse to a host, a cluster, or a data center.
2. From the right-click menu, select **Storage** > **New Datastore**.
3. Select VMFS as the datastore type.
4. Enter the datastore name and if necessary, select the placement location for the datastore.

   The system enforces an 80 character limit for the datastore name.

5. Select the device to use for your datastore.

   Important: The device you select must not have any values displayed in the Snapshot Volume column. If a value is present, the device contains a copy of an existing VMFS datastore. For information on managing datastore copies, see Managing Duplicate VMFS Datastores.

6. Specify the datastore version.

Option	Description
VMFS6	Default format on all hosts that support VMFS6. The ESXi hosts of version 6.0 or earlier cannot recognize the VMFS6 datastore.
VMFS5	VMFS5 datastore supports access by the ESXi hosts of version 6.7 or earlier.

7. Define configuration details for the datastore.

   Note: The required minimum size for a VMFS6 datastore is 2 GB.

   a) Specify partition configuration.

Option	Description
Use all available partitions	Dedicates the entire disk to a single VMFS datastore. If you select this option, all file systems and data currently stored on this device are destroyed.
Use free space	Deploys a VMFS datastore in the remaining free space of the disk.

   b) If the space allocated for the datastore is excessive for your purposes, adjust the capacity values in the Datastore Size field.

   By default, the entire free space on the storage device is allocated.

   c) For VMFS6, specify the block size and define space reclamation parameters. See Space Reclamation Requests from VMFS Datastores.

8. In the Ready to Complete page, review the datastore configuration information and click **Finish**.

The datastore on the SCSI-based storage device is created. It is available to all hosts that have access to the device. After you create the VMFS datastore, you can perform the following tasks:

- Change the capacity of the datastore. See Increase VMFS Datastore Capacity.
- Edit space reclamation settings. See Change Space Reclamation Settings.
- Enable shared vmdk support. See Enable or Disable Support for Clustered Virtual Disks on the VMFS6 Datastore.

Create an NFS Datastore

You can use the **New Datastore** wizard to mount an NFS volume.

- Set up NFS storage environment.
- If you plan to use Kerberos authentication with the NFS 4.1 datastore, make sure to configure the ESXi hosts for Kerberos authentication.

1. In the vSphere Client object navigator, browse to a host, a cluster, or a data center.
2. From the right-click menu, select **Storage** > **New Datastore**.
3. Select NFS as the datastore type and specify an NFS version.
   - NFS 3
   - NFS 4.1

   Important: If multiple hosts access the same datastore, you must use the same protocol on all hosts.

4. Enter the datastore parameters.

Option	Description
Datastore name	The system enforces an 80 character limit for the datastore name.
Folder	The mount point folder name
Server	The server name or IP address. You can use IPv6 or IPv4 formats. With NFS 4.1, you can add multiple IP addresses or server names if the NFS server supports trunking. The ESXi host uses these values to achieve multipathing to the NFS server mount point.

5. Select **Mount NFS read only** if the volume is exported as read-only by the NFS server.
6. To use Kerberos security with NFS 4.1, enable Kerberos and select an appropriate Kerberos model.

Option	Description
Use Kerberos for authentication only (krb5)	Supports identity verification
Use Kerberos for authentication and data integrity (krb5i)	In addition to identity verification, provides data integrity services. These services help to protect the NFS traffic from tampering by checking data packets for any potential modifications.

   If you do not enable Kerberos, the datastore uses the default AUTH_SYS security.
7. If you are creating a datastore at the data center or cluster level, select hosts that mount the datastore.
8. Review the configuration options and click **Finish**.

Create a Virtual Volumes Datastore

You use the **New Datastore** wizard to create a Virtual Volumes datastore.

1. In the vSphere Client object navigator, browse to a host, a cluster, or a data center.
2. From the right-click menu, select **Storage** > **New Datastore**.
3. Select **vVol** as the datastore type.
4. Enter the datastore name and select a backing storage container from the list of storage containers.
   Make sure to use the name that does not duplicate another datastore name in your data center environment.

   If you mount the same Virtual Volumes datastore to several hosts, the name of the datastore must be consistent across all hosts.
5. Select the hosts that require access to the datastore.
6. Review the configuration options and click **Finish**.

After you create the Virtual Volumes datastore, you can perform such datastore operations as renaming the datastore, browsing datastore files, unmounting the datastore, and so on.

You cannot add the Virtual Volumes datastore to a datastore cluster.

Managing Duplicate VMFS Datastores

When a storage device contains a VMFS datastore copy, you can mount the datastore with the existing signature or assign a new signature.

Each VMFS datastore created on a storage device has a unique signature, also called UUID, that is stored in the file system superblock. When the storage device is replicated or its snapshot is taken on the array side, the resulting device copy is identical, byte-for-byte, with the original device. For example, if the original storage device contains a VMFS datastore with UUIDX, the copy appears to contain a datastore copy with the same UUIDX.

In addition to LUN snapshots and replications, certain device operations, such as LUN ID changes, might produce a copy of the original datastore.

ESXi can detect the VMFS datastore copy. You can mount the datastore copy with its original UUID or change the UUID. The process of changing the UUID is called the datastore resignaturing.

Whether you select resignaturing or mounting without resignaturing depends on how the LUNs are masked in the storage environment. If your hosts can see both copies of the LUN, then resignaturing is the optimal method.

Keeping Existing Datastore Signature

If you do not need to resignature a VMFS datastore copy, you can mount it without changing its signature.

You can keep the signature if, for example, you maintain synchronized copies of virtual machines at a secondary site as part of a disaster recovery plan. In the event of a disaster at the primary site, you mount the datastore copy and power on the virtual machines at the secondary site.

Resignaturing a VMFS Datastore Copy

Use datastore resignaturing if you want to retain the data stored on the VMFS datastore copy.

When resignaturing a VMFS copy, ESXi assigns a new signature (UUID) to the copy, and mounts the copy as a datastore distinct from the original. All references to the original signature in virtual machine configuration files are updated.

When you perform datastore resignaturing, consider the following points:

- Datastore resignaturing is irreversible.
- After resignaturing, the storage device replica that contained the VMFS copy is no longer treated as a replica.
- A spanned datastore can be resignatured only if all its extents are online.
- The resignaturing process is fault tolerant. If the process is interrupted, you can resume it later.
- You can mount the new VMFS datastore without a risk of its UUID conflicting with UUIDs of any other datastore from the hierarchy of device snapshots.

Mount a VMFS Datastore Copy

Use datastore resignaturing if you want to retain the data stored on the VMFS datastore copy. If you do not need to resignature the VMFS datastore copy, you can mount it without changing its signature.

- Perform a storage rescan on your host to update the view of storage devices presented to the host.
- Unmount the original VMFS datastore that has the same UUID as the copy you plan to mount. You can mount the VMFS datastore copy only if it does not collide with the original VMFS datastore.

1. In the vSphere Client object navigator, browse to a host, a cluster, or a data center.
2. From the right-click menu, select **Storage** > **New Datastore**.
3. Select VMFS as the datastore type.
4. Enter the datastore name and if necessary, select the placement location for the datastore.
5. From the list of storage devices, select the device that has a specific value displayed in the Snapshot Volume column.

   The value present in the Snapshot Volume column indicates that the device is a copy that contains a copy of an existing VMFS datastore.

6. Mount the datastore.

Option	Description
Mount with resignaturing	Under **Mount Options**, select **Assign a New Signature** and click **Next** .
Mount without resignaturing	Under Mount Options, select **Keep Existing Signature**.

7. Review the datastore configuration information and click **Finish**.

Increase VMFS Datastore Capacity

You can increase the capacity of a VMFS datastore. Additional capacity might be required when you add virtual machines to the datastore, or when the virtual machines running on the datastore require more space.

You can increase the datastore capacity if the host storage meets one of the following conditions:

- The backing device for the existing datastore has enough free space.
- You added new storage devices to the host.

If a shared datastore has powered on virtual machines and becomes 100% full, you can increase the datastore capacity. You can perform this action only from the host where the powered on virtual machines are registered.
Depending on your storage configuration, you can use one of the following methods to increase the datastore capacity. You do not need to power off virtual machines when using either method of increasing the datastore capacity.

Expand an Existing Datastore	Increase the size of an expandable datastore. The datastore is considered expandable when the backing storage device has free space immediately after the datastore extent.
Add an Extent	Increase the capacity of an existing VMFS datastore by adding new storage devices to the datastore. The datastore can span over multiple storage devices, yet appear as a single volume. The spanned VMFS datastore can use any or all its extents at any time. It does not need to fill up a particular extent before using the next one. **Note:** Datastores that support only the hardware assisted locking, also called the atomic test and set (ATS) mechanism, cannot span over non-ATS devices. For more information, see VMFS Locking Mechanisms.

1. In the vSphere Client, navigate to the datastore.
2. Select **Increase Datastore Capacity** from the datastore right-click menu.
3. Select a device from the list of storage devices.
   Your selection depends on whether an expandable storage device is available.

Option	Description
To expand an existing datastore extent	Select the device for which the Expandable column reads YES.
To add an extent	Select the device for which the Expandable column reads NO.

4. Review the **Partition Layout** to see the available configurations.
5. Select a configuration option from the bottom panel.
   Depending on the current layout of the disk and on your previous selections, the menu items you see might vary.

Menu Item	Description
Use free space to expand the datastore	Expands an existing extent to a required capacity.
Use free space	Deploys an extent in the remaining free space of the disk. This menu item is available only when you are adding an extent.

Menu Item	Description
Use all available partitions	Dedicates the entire disk to a single extent. This menu item is available only when you are adding an extent and when the disk you are formatting is not blank. The disk is reformatted, and the datastores and any data that it contains are erased.

6. Set the capacity for the extent.
   The minimum extent size is 1.3 GB. By default, the entire free space on the storage device is available.
7. Click **Next**.
8. Review the proposed layout and the new configuration of your datastore, and click **Finish**.

Enable or Disable Support for Clustered Virtual Disks on the VMFS6 Datastore

If you plan to use a virtual disk in Windows Server Failover Clustering (WSFC) configurations, your VMFS6 datastore must support clustered virtual disks. Use the vSphere Client to enable the clustered disk support.

Follow these guidelines when you use a datastore for clustered virtual disks:

- The storage array must support the ATS, Write Exclusive – All Registrant (WEAR) SCSI-3 reservation type.
- ESXi supports only Fibre Channel arrays for this type of configurations.
- Only VMFS6 datastores support clustered disks. The datastores you use cannot be expanded or span multiple extents.
- Storage devices must be claimed by the NMP. ESXi does not support third-party plug-ins (MPPs) in the clustered virtual disk configurations.
- Make sure that the virtual disks you use for clustering are in the Thick Provision Eager Zeroed format.

For information on the use of clustered virtual disks in VM clusters, see the *Setup for Windows Server Failover Clustering* documentation.

1. In the vSphere Client, navigate to the datastore.
2. Click the **Configure** tab, and click **General**.
3. Under **Datastore Capabilities**, click one of the following options next to the **Clustered VMDK** item.

Option	Description
Enable	To enable support for clustered virtual disks on the datastore. After you enable the support, you can place the clustered virtual disks on this VMFS datastore.
Disable	To disable the support. Before disabling, make sure to power off all virtual machines with the clustered virtual disks.

4. Confirm your configuration.

Administrative Operations for Datastores

After creating datastores, you can perform several administrative operations on the datastores. Certain operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.

Change Datastore Name

Use the vSphere Client to change the name of an existing datastore. You can rename the datastore that has virtual machines running on it without any negative impact.

Note: If the host is managed by vCenter Server, you cannot rename the datastore by directly accessing the host from the VMware Host Client. You must rename the datastore from vCenter Server.

1. In the vSphere Client, navigate to the datastore.
2. Right-click the datastore to rename, and select **Rename**.
3. Enter a new datastore name.
   The system enforces an 80 character limit for the datastore name.

The new name appears on all hosts that have access to the datastore.

Unmount Datastores

When you unmount a datastore, it remains intact, but can no longer be seen from the hosts that you specify. The datastore continues to appear on other hosts, where it remains mounted.

When appropriate, before unmounting datastores, make sure that the following prerequisites are met:

- No virtual machines reside on the datastore.
- Storage DRS does not manage the datastore.
- Storage I/O Control is disabled for this datastore.

Do not perform any configuration operations that might result in I/O to the datastore while the unmounting is in progress.
Note: Make sure that the datastore is not used by vSphere HA Heartbeating. vSphere HA Heartbeating does not prevent you from unmounting the datastore. However, if the datastore is used for heartbeating, unmounting it might cause the host to fail and restart any active virtual machine.

1. In the vSphere Client, navigate to the datastore.
2. Right-click the datastore and select **Unmount Datastore**.
3. If the datastore is shared, select the hosts from which to unmount the datastore.
4. Confirm that you want to unmount the datastore.

After you unmount a VMFS datastore from all hosts, the datastore is marked as inactive. If you unmount an NFS or a Virtual Volumes datastore from all hosts, the datastore disappears from the inventory. You can mount the unmounted VMFS datastore. To mount the NFS or Virtual Volumes datastore that has been removed from the inventory, use the New Datastore wizard.

If you unmounted the VMFS datastore as a part of a storage removal procedure, you can now detach the storage device that is backing the datastore. See Detach Storage Devices.

Mount Datastores

You can mount a datastore you previously unmounted. You can also mount a datastore on additional hosts, so that it becomes a shared datastore.

A VMFS datastore that has been unmounted from all hosts remains in inventory, but is marked as inaccessible. See Unmount Datastores.

You can use this task to mount the VMFS datastore to a specified host or multiple hosts.

If you have unmounted an NFS or a Virtual Volumes datastore from all hosts, the datastore disappears from the inventory. To mount the NFS or Virtual Volumes datastore that has been removed from the inventory, use the New Datastore wizard.

A datastore of any type that is unmounted from some hosts while being mounted on others, is shown as active in the inventory.

1. In the vSphere Client, navigate to the datastore.
2. Right-click the datastore to mount and select one of the following options:
   - **Mount Datastore**
   - **Mount Datastore on Additional Hosts**

   Whether you see one or another option depends on the type of datastore you use.
3. Select the hosts that should access the datastore and click **OK**.
4. To list all hosts that share the datastore, navigate to the datastore, and click the **Hosts** tab.

Remove VMFS Datastores

You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, it is destroyed and disappears from all hosts that have access to the datastore.

- Remove or migrate all virtual machines from the datastore.
- Unmount the datastore from all hosts.
- Disable Storage DRS for the datastore. For more information, see Activate and Deactivate Storage DRS.
- Disable Storage I/O Control for the datastore. For more information, see Enable Storage I/O Control.
- Make sure that the datastore is not used for vSphere HA heartbeating. For more information, see Configure Heartbeat Datastores.

Note: The delete operation for the datastore permanently deletes all files associated with virtual machines on the datastore. Although you can delete the datastore without unmounting, it is preferable that you unmount the datastore first.

1. In the vSphere Client, navigate to the datastore.
2. Right-click the datastore to remove, and select **Delete Datastore**.
3. Confirm that you want to remove the datastore.

Use Datastore Browser

Use the datastore file browser to manage contents of your datastores. You can browse folders and files that are stored on the datastore. You can also use the browser to upload files and perform administrative tasks on your folders and files.

1. Open the datastore browser.
   a) Display the datastore in the inventory.
   b) Right-click the datastore and select **Browse Files**.
2. Explore the contents of the datastore by navigating to existing folders and files.
3. Perform administrative tasks by using the icons and options.

Icons and Options	Descriptions
Upload Files	Upload a file to the datastore.
Upload Folder (Available only in the vSphere Client)	Upload a folder to the datastore.
Download	Download from the datastore.
New Folder	Create a folder on the datastore.

Icons and Options	Descriptions
Copy to	Copy selected folders or files to a new location, either on the same datastore or on a different datastore.
Move to	Move selected folders or files to a new location, either on the same datastore or on a different datastore.
Rename to	Rename selected files.
Delete	Delete selected folders or files.
Inflate	Convert a selected thin virtual disk to thick. This option applies only to thin-provisioned disks.

Upload Files or Folders to Datastores

Use the datastore file browser to upload files to datastores on the ESXi host. If you use the vSphere Client, you can also upload folders.

Required privilege:**Datastore** > **Browse Datastore**

In addition to their traditional use as storage for virtual machines files, datastores can serve to store data or files related to virtual machines. For example, you can upload ISO images of operating systems from a local computer to a datastore on the host. You then use these images to install guest operating systems on the new virtual machines.

Note: You cannot upload files directly to the Virtual Volumes datastores. You must first create a folder on the Virtual Volumes datastore, and then upload the files into the folder. The created folders in Virtual Volumes datastores for block storage have a limited storage capacity space of 4GB. The Virtual Volumes datastore supports direct uploads of folders.

1. Open the datastore browser.
   a) Display the datastore in the inventory.
   b) Right-click the datastore and select **Browse Files**.
2. Optional: Create a folder to store the file or folder.
3. Upload the file or folder.

Option	Description
Upload a file	1. Select the target folder and click **Upload Files**. 2. Locate the item to upload on the local computer and click **Open**.
Upload a folder (available only in the vSphere Client)	1. Select the datastore or the target folder and click **Upload Folders**. 2. Locate the item to upload on the local computer and click **Ok**.

4. Refresh the datastore file browser to see the uploaded files or folders on the list.

Download Files from Datastores

Use the datastore file browser to download files from the datastore available on your ESXi host to your local computer.

- Required privilege:**Datastore** > **Browse Datastore**

- Privileges when a VM is encrypted:**Cryptographic operations** > **Decrypt** and**Cryptographic operations** > **Direct Access**

1. Open the datastore browser.
   a) Display the datastore in the inventory.
   b) Right-click the datastore and select **Browse Files**.
2. Navigate to the file to download and click **Download**.
3. Follow the prompts to save the file to your local computer.

Move or Copy Datastore Folders or Files

Use the datastore browser to move or copy folders or files to a new location, either on the same datastore or on a different datastore.

Required privilege: **Datastore** > **Browse Datastore**

Note: Virtual disk files are moved or copied without format conversion. If you move a virtual disk to a datastore that belongs to a host different from the source host, you might need to convert the virtual disk. Otherwise, you might not be able to use the disk.

You cannot copy VM files across vCenter Servers.

1. Open the datastore browser.
   a) Display the datastore in the inventory.
   b) Right-click the datastore and select **Browse Files**.
2. Browse to an object you want to move or copy, either a folder or a file.
3. Select the object and click **Move to** or **Copy to**.
4. Specify the destination location.
5. Optional: Select **Overwrite files and folders with matching names at the destination**.
6. Click **OK**.

Rename Datastore Files

Use the datastore browser to rename files.

Required privilege: **Datastore** > **Browse Datastore**

1. Open the datastore browser.
   a) Display the datastore in the inventory.
   b) Right-click the datastore and select **Browse Files**.
2. Browse to a file you want to rename.
3. Select the file and click **Rename to**.
4. Specify the new name and click **OK**.

Inflate Thin Virtual Disks

If you created a virtual disk in the thin format, you can change the format to thick.

- Make sure that the datastore where the virtual machine resides has enough space.
- Make sure that the virtual disk is thin.
- Remove snapshots.

- Power off your virtual machine.

You use the datastore browser to inflate the thin virtual disk.

1. In the vSphere Client, navigate to the folder of the virtual disk you want to inflate.
   a) Navigate to the virtual machine.
   b) Click the **Datastores** tab.
      The datastore that stores the virtual machine files is listed.
   c) Right-click the datastore and select **Browse Files**.
      The datastore browser displays contents of the datastore.
2. Expand the virtual machine folder and browse to the virtual disk file that you want to convert.
   The file has the `.vmdk` extension and is marked with the virtual disk ( ) icon.
3. Select the virtual disk file and click **Inflate**.

   Note: The option might not be available if the virtual disk is thick or when the virtual machine is running.

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Turn Off Storage Filters

When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices.

Before you change the device filters, consult with the VMware support team.

1. Browse to the vCenter Server instance.
2. Click the **Configure** tab.
3. Under **Settings**, click **Advanced Settings**, and click **EDIT SETTINGS**.
4. Specify the filter to turn off.
   In the **Name** and **Value** text boxes at the bottom of the page, enter appropriate information.

Name	Value
config.vpxd.filter.vmfsFilter	False
config.vpxd.filter.rdmFilter	False
config.vpxd.filter.sameHostsAndTransportsFilter	False
config.vpxd.filter.hostRescanFilter	False **Note:** If you turn off this filter, your hosts continue to perform a rescan each time you present a new LUN to a host or a cluster.

5. Click **ADD**, and click **SAVE** to save your changes.
   You are not required to restart the vCenter Server system.

Storage Filtering

vCenter Server provides storage filters to help you avoid storage device corruption or performance degradation that might be caused by an unsupported use of storage devices. These filters are available by default.

Table 219: Storage Filters

Filter Name	Description
config.vpxd.filter.vmfsFilter (VMFS Filter)	Filters out storage devices, or LUNs, that are already used by a VMFS datastore on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with another VMFS datastore or to be used as an RDM.
config.vpxd.filter.rdmFilter (RDM Filter)	Filters out LUNs that are already referenced by an RDM on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with VMFS or to be used by a different RDM. For your virtual machines to access the same LUN, the virtual machines must share the same RDM mapping file. For information about this type of configuration, see the *vSphere Resource Management* documentation.
config.vpxd.filter.sameHostsAndTransportsFilter (Same Hosts and Transports Filter)	Filters out LUNs ineligible for use as VMFS datastore extents because of host or storage type incompatibility. Prevents you from adding the following LUNs as extents: • LUNs not exposed to all hosts that share the original VMFS datastore. • LUNs that use a storage type different from the one the original VMFS datastore uses. For example, you cannot add a Fibre Channel extent to a VMFS datastore on a local storage device.
config.vpxd.filter.hostRescanFilter (Host Rescan Filter)	Automatically rescans and updates VMFS datastores after you perform datastore management operations. The filter helps provide a consistent view of all VMFS datastores on all hosts managed by vCenter Server. **Note:** If you present a new LUN to a host or a cluster, the hosts automatically perform a rescan no matter whether you have the Host Rescan Filter on or off.

Set Up Dynamic Disk Mirroring

Typically, you cannot use LUN manager software on virtual machines to mirror virtual disks. However, if your Microsoft Windows virtual machines support dynamic disks, you can mirror virtual disks across two SAN LUNs. Mirroring helps you to protect the virtual machines from an unplanned storage device loss.

- Use a Windows virtual machine that supports dynamic disks.
- Required privilege: **Virtual machine** > **Configuration** > **Settings**

1. Create a virtual machine with two virtual disks.
   Place the disks on different datastores.
2. Log in to your virtual machine and configure the disks as dynamic mirrored disks.
   See Microsoft documentation.
3. After the disks synchronize, power off the virtual machine.
4. Change virtual machine settings to enable the dynamic disk mirroring.
   a) Right-click the virtual machine and select **Edit Settings**.
   b) Click the **VM Options** tab and expand the **Advanced** menu.
   c) Click **Edit Configuration** next to Configuration Parameters.
   d) Click **Add Configuration Params** and add the following parameters:
   Replace # with the boot device SCSI bus controller ID number. By default, it is set to 0.

Name	Value
`scsi#.returnNoConnectDuringAPD`	True

Name	Value
`scsi#.returnBusyOnNoConnectStatus`	False

e) If you use ESXi version 6.7 or later, include an additional parameter for each virtual disk participating in the software RAID-1 configuration.

The parameter prevents guest OS I/O failures when a storage device fails.

Replace `#` with the boot device SCSI bus controller ID number. By default, it is set to 0.

Name	Value
`scsi#:1.passthruTransientErrors`	True
`scsi#:2.passthruTransientErrors`	True

f) Click **OK**.

Collecting Diagnostic Information for ESXi Hosts on a VMFS Datastore

During a host failure, ESXi must be able to save diagnostic information to a preconfigured location for diagnostic and technical support purposes.

Typically, a partition to collect diagnostic information, also called a core dump, is created on a local storage device during ESXi installation. You can also configure ESXi Dump Collector keep core dumps on a network server. For information on setting up ESXi Dump Collector, see the *VMware ESXi Installation and Setup* documentation.

Another option is to use a file on a VMFS datastore to collect the diagnostic information.

Set Up a File as Core Dump Location

If the size of your available core dump partition is insufficient, you can configure ESXi to use a file on a VMFS datastore for diagnostic information.

- Make sure that the amount of available space in the datastore for a core dump file is twice as large as the recommended file size. For more information, see the Knowledge Base article 2058416.
- Install ESXCLI. See Getting Started with ESXCLI. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Note: VMFS datastores on software iSCSI do not support core dump files.

1. Create a VMFS datastore core dump file by running the following command:

   ```
   esxcli system coredump file add
   ```

   The command takes the following options, but they are not required and can be omitted:

Option	Description
`--auto | -a`	Automatically create a file if none found.
`--datastore | -d` ***`datastore_UUID or datastore_name`***	Specify the datastore for the dump file. If not provided, the system selects a datastore of sufficient size.
`--enable | -e`	Enable the diagnostic file after creation.
`--file | -f` ***`file_name`***	Specify the file name of the dump file. If not provided, the system creates a unique name for the file.
`--size |-s` ***`file_size_MB`***	Set the size in MB of the dump file. If not provided, the system creates a file of the size appropriate for the memory installed in the host.

2. Verify that the file has been created:

   ```
   esxcli system coredump file list
   ```

   You can see the output similar to the following:

   ```
   Path                                          Active Configured Size
   --------------------------------------------- ------ ---------- ---------
   /vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile false  false      104857600
   ```

3. Activate the core dump file for the host:

   ```
   esxcli system coredump file set
   ```

   The command takes the following options:

Option	Description
--enable |-e	Enable or disable the dump file. This option cannot be specified when unconfiguring the dump file.
--path | -p	The path of the core dump file to use. The file must be pre-allocated.
--smart | -s	This flag can be used only with **--enable | -e=true**. It causes the file to be selected using the smart selection algorithm. For example, `esxcli system coredump file set --smart --enable true`
--unconfigure | -u	Unconfigure the current VMFS dump file.

4. Verify that the core dump file is active and configured:

   ```
   esxcli system coredump file list
   ```

   The output similar to the following indicates that the core dump file is active and configured:

   ```
   Path                                          Active Configured Size
   --------------------------------------------- ------ ---------- ---------
   /vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile True   True       104857600
   ```

For information about other commands you can use to manage the core dump files, see the *ESXCLI Reference* documentation.

Related Links

Deactivate and Delete a Core Dump File on page 2540

Deactivate a configured core dump file and, if needed, remove it from the VMFS datastore.

Deactivate and Delete a Core Dump File

Deactivate a configured core dump file and, if needed, remove it from the VMFS datastore.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

You can temporarily deactivate the core dump file. If you do not plan to use the deactivated file, you can remove it from the VMFS datastore. To remove the file that has not been deactivated, you can use the `esxcli system coredump file remove` command with the `--force | -F` parameter.

1. List the core dump files:

   ```
   esxcli system coredump file list
   ```

2. Deactivate the core dump file by running the following command:

   ```
   esxcli system coredump file set --unconfigure | -u
   ```

3. Remove the file from the VMFS datastore:

   ```
   esxcli system coredump file remove --file | -f file_name
   ```

   The command takes the following options:

Option	Description
--file | -f	Enter the name of the dump file to be removed. If you do not enter the name, the command removes the default configured core dump file.
--force | -F	Deactivate and unconfigure the dump file being removed. This option is required if the file has not been previously deactivated and is active.

The core dump file becomes disabled and is removed from the VMFS datastore.

Related Links

Set Up a File as Core Dump Location on page 2539

If the size of your available core dump partition is insufficient, you can configure ESXi to use a file on a VMFS datastore for diagnostic information.

Checking Metadata Consistency with VOMA

Use vSphere On-disk Metadata Analyzer (VOMA) to identify and fix incidents of metadata corruption that affect file systems or underlying logical volumes.

You can check metadata consistency when you experience problems with a VMFS datastore or a virtual flash resource. For example, perform a metadata check if one of the following occurs:

- You experience storage outages.
- After you rebuild RAID or perform a disk replacement.
- You see metadata errors in the `vmkernel.log` file similar to the following:

  ```
  cpu11:268057)WARNING: HBX: 599: Volume 50fd60a3-3aae1ae2-3347-0017a4770402 ("<Datastore_name>") may be
   damaged on disk. Corrupt heartbeat detected at offset 3305472: [HB state 0 offset 6052837899185946624 gen
   15439450 stampUS 5 $
  ```

- You are unable to access files on a VMFS.
- You see corruption being reported for a datastore in events tabs of vCenter Server.

To check metadata consistency, run VOMA from the CLI of an ESXi host. VOMA can be used to check and fix minor inconsistency issues for a VMFS datastore or logical volumes that back the VMFS datastore.

VOMA can check and fix the following items.

Table 220: VOMA Functions

VOMA Functions	Description
Metadata check and fix	Examples of metadata check and fix include, but are not limited to, the following: • Validation of VMFS volume header for basic metadata consistency. • Checking consistency of VMFS resource files (system file). • Checking the pathname and connectivity of all files.
Affinity metadata check and fix	To enable the affinity check for VMFS6, use the `-a|--affinityChk` option. Several examples of affinity metadata check and fix include the following: • Affinity flags in resource types and FS3_ResFileMetadata. • Validation of affinity flags in SFB RC meta (FS3_ResourceClusterMDVMFS6).

VOMA Functions	Description
	• Validation of all entries in the affinityInfo entries in rcMeta of RC, including the overflow key, to make sure that no invalid entries exist. Checking for missing entries.
Directory validation	VOMA can detect and correct the following errors: • Directory hash block corruption. • Alloc map corruption. • Link blocks corruptions. • Directory entry block corruptions. Based on the nature of the corruption, VOMA can either fix only the corrupted entries or fully reconstruct the hash block, alloc map blocks and link blocks.
Lost and found files	During a filesystem check, VOMA can find files that are not referenced anywhere in the filesystem. These orphaned files are valid and complete, but do not have a name or directory entry on the system. If VOMA encounters orphaned files during scanning, it creates a directory named lost+found at the root of the volume to store the orphaned files. The names of the files use the `File`*`sequence-number`* format.

Command options that the VOMA tool takes include the following.

Table 221: VOMA Command Options

Command Option	Description	
`-m|--module`	The modules to run include the following:	
	`vmfs`	If you do not specify the name of the module, this option is used by default. You can check the VMFS file systems and the file systems that back virtual flash resources. If you specify this module, minimal checks are performed for LVM as well.
	`lvm`	Check logical volumes that back the VMFS datastores.
	`ptbl`	Check and validate VMFS partitions, such as MBR or GPT. If no partition exists, determine whether partitions should exist.
`-f|--func`	Functions to be performed include the following:	
	`query`	List functions supported by module.
	`check`	Check for errors.
	`fix`	Check and fix errors.
	`dump`	Collect metadata dump.
`-a|--affinityChk`	Include affinity-related check and fix for VMFS6.	
`-d|--device`	Indicate the device or disk to inspect. Make sure to provide the absolute path to the device partition backing the VMFS datastore. If the datastore spans multiple devices, provide the UUID of the head extent. For example, `voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x` If you use the `-x|--extractDump` command, enter multiple device paths, with a partition qualifier, separated with a comma. The number of device paths you enter equals the number of spanned devices.	

Command Option	Description
-b|--blockSize	Indicate the disk block size.
-s|--logfile	Specify the path to log file to output the results.
-x|--extractDump	Extract the collected dump using VOMA.
-D|--dumpfile	Indicate the dump file to save the collected metadata dump.
-v|--version	Display the version of VOMA.
-h|--help	Display the help message for the VOMA command.
-Y	Indicate that you run VOMA without using PE tables for address resolution.
-Z| --file	Indicate that you run VOMA on extracted device files.

Use VOMA to Check Metadata Consistency

The task demonstrates how to use VOMA to check VMFS metadata consistency. VOMA can be used to check and fix minor inconsistency issues for a VMFS datastore or a virtual flash resource. Run VOMA from the CLI of an ESXi host.

Power off any virtual machines that are running or migrate them to a different datastore.

1. Obtain the name and partition number of the device that backs the VMFS datastore that you want to check.

   ```
   #esxcli storage vmfs extent list
   ```

   The Device Name and Partition columns in the output identify the device. For example:

   ```
   Volume Name  .....  Device Name                            Partition
   1TB_VMFS6    .....  naa.xxxx                                  3
   ```

2. Check for VMFS errors.

   Provide the absolute path to the device partition that backs the VMFS datastore, and provide a partition number with the device name. For example:

   ```
   # voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x
   ```

   The output lists possible errors. For example, the following output indicates that the heartbeat address is invalid.

   ```
   XXXXXXXXXXXXXXXXXXXXXXX
   Phase 2: Checking VMFS heartbeat region
    ON-DISK ERROR: Invalid HB address
   Phase 3: Checking all file descriptors.
   Phase 4: Checking pathname and connectivity.
   Phase 5: Checking resource reference counts.

   Total Errors Found:          1
   ```

Configuring VMFS Pointer Block Cache

Pointer blocks, also called indirection blocks, are file system resources that contain addresses to VMFS file blocks. When you open a `vmdk` file on an ESXi host, pointer blocks related to that file are stored in the pointer block cache. The size of the pointer block cache is a configurable parameter.

The pointer block cache is a host-wide cache that is independent from VMFS. The cache is shared across all datastores that are accessed from the same ESXi host.

The size of the pointer block cache is controlled by `/VMFS3/MinAddressableSpaceTB` and `/VMFS3/MaxAddressableSpaceTB`. You can configure the minimum and maximum sizes on each ESXi host.

/VMFS3/MinAddressableSpaceTB	The minimum value is minimum amount of memory that the system guarantees to the pointer block cache. For example, 1 TB

	of open file space requires approximately 4 MB of memory. Default value is 10 TB.
/VMFS3/MaxAddressableSpaceTB	The parameter defines the maximum limit of pointer blocks that can be cached in memory. Default value is 32 TB. Maximum value is 128 TB. Typically, the default value of the `/VMFS3/MaxAddressableSpaceTB` parameter is adequate. However, as the size of the open vmdk files increases, the number of pointer blocks related to those files also increases. If the increase causes any performance degradation, you can adjust the parameter to its maximum value to provide more space for the pointer block cache. Base the maximum size of the pointer block cache on the working set, or the active pointer blocks required.
Pointer Block Eviction	The `/VMFS3/MaxAddressableSpaceTB` parameter also controls the growth of the pointer block cache. When the size of the pointer block cache approaches the configured maximum size, a pointer block eviction process starts. The mechanism leaves active pointer blocks, but removes non-active or less active blocks from the cache, so that space can be reused.

To change the values for the pointer block cache, use the **Advanced System Settings** dialog box of the vSphere Client or the `esxcli system settings advanced set -o` command.

You can use the `esxcli storage vmfs pbcache` command to obtain information about the size of the pointer block cache and other statistics. This information assists you in adjusting minimum and maximum sizes of the pointer block cache, so that you can get maximum performance.

Obtain Information for VMFS Pointer Block Cache

You can get information about VMFS pointer block cache use. This information helps you understand how much space the pointer block cache consumes. You can also determine whether you must adjust the minimum and maximum sizes of the pointer block cache.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To obtain or reset the pointer block cache statistics, use the following command:

`esxcli storage vmfs pbcache`

Option	Description
`get`	Get VMFS pointer block cache statistics.
`reset`	Reset the VMFS pointer block cache statistics.

Getting Statistics for Pointer Block Cache

```
#esxcli storage vmfs pbcache get
   Cache Capacity Miss Ratio: 0 %
   Cache Size: 0 MiB
   Cache Size Max: 132 MiB
   Cache Usage: 0 %
   Cache Working Set: 0 TiB
   Cache Working Set Max: 32 TiB
   Vmfs Heap Overhead: 0 KiB
   Vmfs Heap Size: 23 MiB
   Vmfs Heap Size Max: 256 MiB
```

Change the Size of the Pointer Block Cache

You can adjust the minimum and maximum sizes of the pointer block cache.

CAUTION: Changing advanced options is considered unsupported. Typically, the default settings produce the optimum result. Change the advanced options only when you get specific instructions from VMware technical support or a knowledge base article.

1. Browse to the host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. In Advanced System Settings, select the appropriate item.

Option	Description
`VMFS3.MinAddressableSpaceTB`	Minimum size of all open files that VMFS cache guarantees to support.
`VMFS3.MaxAddressableSpaceTB`	Maximum size of all open files that VMFS cache supports before eviction starts.

5. Click the **Edit** button and change the value.
6. Click **OK**.

Use the esxcli Command to Change the Pointer Block Cache

You can also use the `esxcli system settings advanced set -o` to modify the size of the pointer block cache. The following example describes how to set the size to its maximum value of 128 TB.

1. To change the value of `/VMFS3/MaxAddressableSpaceTB` to 128 TB, enter the following command:
   ```
   # esxcli system settings advanced set -i 128 -o /VMFS3/MaxAddressableSpaceTB
   ```
2. To confirm that the value is set correctly, enter this command:
   ```
   # esxcli system settings advanced list -o /VMFS3/MaxAddressableSpaceTB
   ```

Understanding Multipathing and Failover

To maintain a constant connection between a host and its storage, ESXi supports multipathing. With multipathing, you can use more than one physical path that transfers data between the host and an external storage device.

If a failure of any element in the SAN network, such as an adapter, switch, or cable, occurs, ESXi can switch to another viable physical path. This process of path switching to avoid failed components is known as path failover.

In addition to path failover, multipathing provides load balancing. Load balancing is the process of distributing I/O loads across multiple physical paths. Load balancing reduces or removes potential bottlenecks.

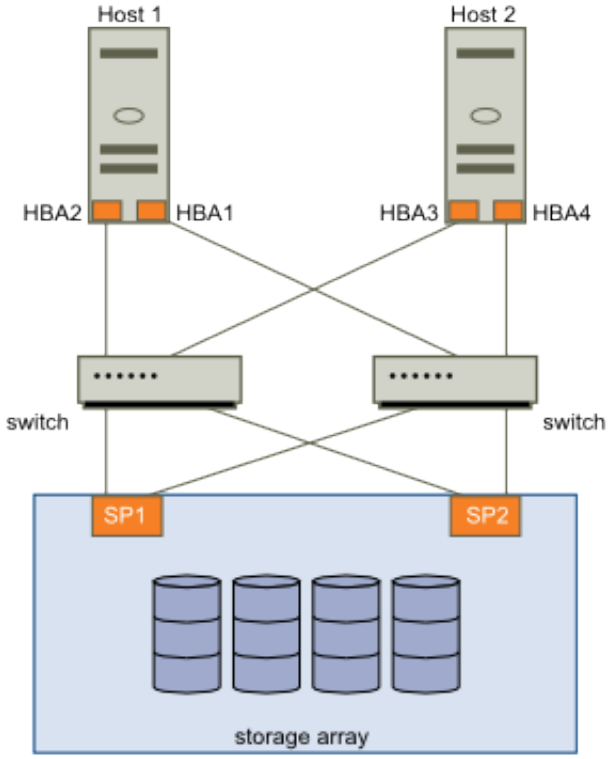
Note: Virtual machine I/O might be delayed for up to 60 seconds while path failover takes place. With these delays, the SAN can stabilize its configuration after topology changes. In general, the I/O delays might be longer on active-passive arrays and shorter on active-active arrays.

Failovers with Fibre Channel

To support multipathing, your host typically has two or more HBAs available. This configuration supplements the SAN multipathing configuration. Generally, the SAN multipathing provides one or more switches in the SAN fabric and one or more storage processors on the storage array device itself.

In the following illustration, multiple physical paths connect each server with the storage device. For example, if HBA1 or the link between HBA1 and the FC switch fails, HBA2 takes over and provides the connection. The process of one HBA taking over for another is called HBA failover.

Figure 74: Multipathing and Failover with Fibre Channel



Similarly, if SP1 fails or the links between SP1 and the switches breaks, SP2 takes over. SP2 provides the connection between the switch and the storage device. This process is called SP failover. VMware ESXi supports both HBA and SP failovers.

Host-Based Failover with iSCSI

When setting up your ESXi host for multipathing and failover, you can use multiple iSCSI HBAs or combine multiple NICs with the software iSCSI adapter.

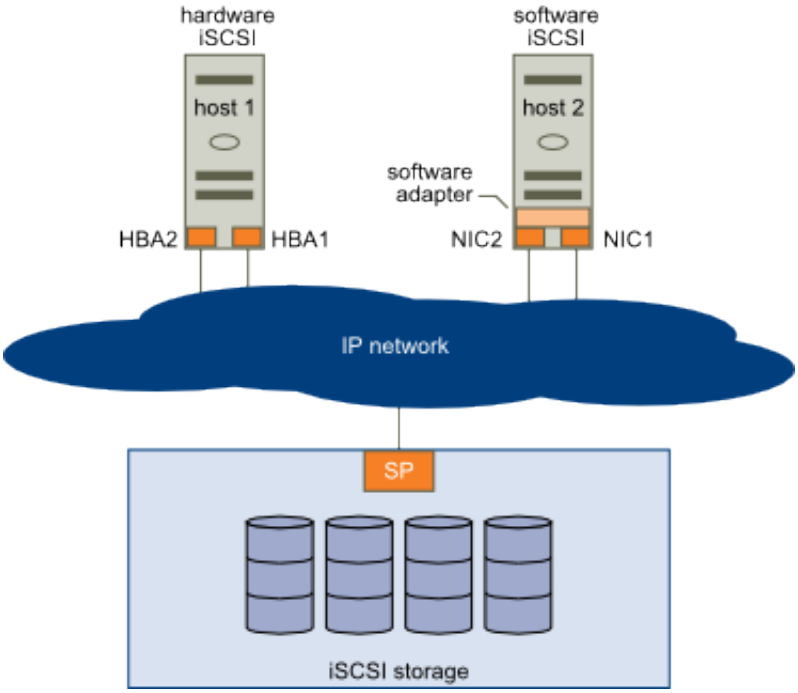
For information on different types of iSCSI adapters, see iSCSI Initiators.

When you use multipathing, specific considerations apply.

- ESXi does not support multipathing when you combine an independent hardware adapter with software iSCSI or dependent iSCSI adapters in the same host.
- Multipathing between software and dependent adapters within the same host is supported.
- On different hosts, you can mix both dependent and independent adapters.

The following illustration shows multipathing setups possible with different types of iSCSI initiators.

Figure 75: Host-Based Path Failover



Hardware iSCSI and Failover

With hardware iSCSI, the host typically has two or more hardware iSCSI adapters. The host uses the adapters to reach the storage system through one or more switches. Alternatively, the setup might include one adapter and two storage processors, so that the adapter can use different paths to reach the storage system.

On the illustration, Host1 has two hardware iSCSI adapters, HBA1 and HBA2, that provide two physical paths to the storage system. Multipathing plug-ins on your host, whether the VMkernel NMP or any third-party MPPs, have access to the paths by default. The plug-ins can monitor health of each physical path. If, for example, HBA1 or the link between HBA1 and the network fails, the multipathing plug-ins can switch the path over to HBA2.

Software iSCSI and Failover

With software iSCSI, as shown on Host 2 of the illustration, you can use multiple NICs that provide failover and load balancing capabilities for iSCSI connections.

Multipathing plug-ins do not have direct access to physical NICs on your host. As a result, for this setup, you first must connect each physical NIC to a separate VMkernel port. You then associate all VMkernel ports with the software iSCSI initiator using a port binding technique. Each VMkernel port connected to a separate NIC becomes a different path that the iSCSI storage stack and its storage-aware multipathing plug-ins can use.

For information about configuring multipathing for software iSCSI, see Setting Up Network for iSCSI and iSER.

Array-Based Failover with iSCSI

Some iSCSI storage systems manage path use of their ports automatically and transparently to ESXi.

When using one of these storage systems, your host does not see multiple ports on the storage and cannot choose the storage port it connects to. These systems have a single virtual port address that your host uses to initially communicate. During this initial communication, the storage system can redirect the host to communicate with another port on the

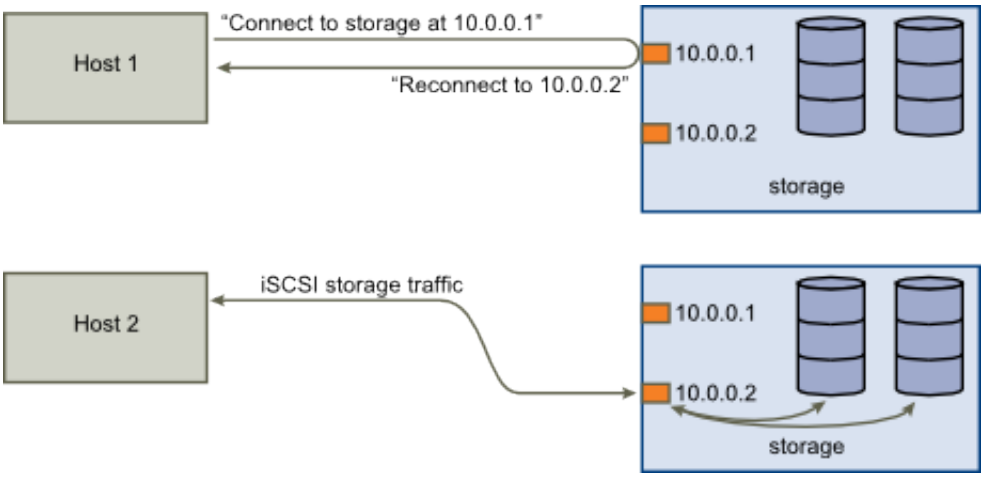
storage system. The iSCSI initiators in the host obey this reconnection request and connect with a different port on the system. The storage system uses this technique to spread the load across available ports.

If the ESXi host loses connection to one of these ports, it automatically attempts to reconnect with the virtual port of the storage system, and should be redirected to an active, usable port. This reconnection and redirection happens quickly and generally does not disrupt running virtual machines. These storage systems can also request that iSCSI initiators reconnect to the system, to change which storage port they are connected to. This allows the most effective use of the multiple ports.

The Port Redirection illustration shows an example of port redirection. The host attempts to connect to the 10.0.0.1 virtual port. The storage system redirects this request to 10.0.0.2. The host connects with 10.0.0.2 and uses this port for I/O communication.

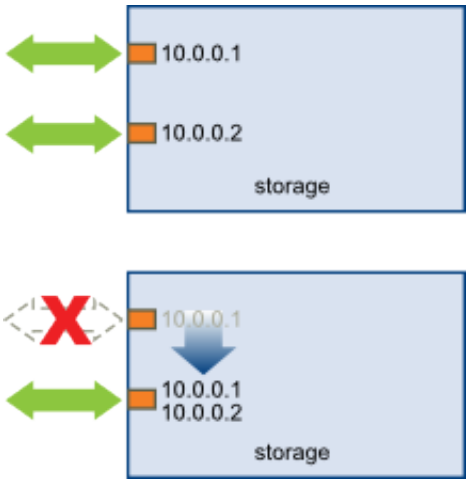
Note: The storage system does not always redirect connections. The port at 10.0.0.1 could be used for traffic, also.

Figure 76: Port Redirection



If the port on the storage system that is acting as the virtual port becomes unavailable, the storage system reassigns the address of the virtual port to another port on the system. Port Reassignment shows an example of this type of port reassignment. In this case, the virtual port 10.0.0.1 becomes unavailable and the storage system reassigns the virtual port IP address to a different port. The second port responds to both addresses.

Figure 77: Port Reassignment



With this form of array-based failover, you can have multiple paths to the storage only if you use multiple ports on the ESXi host. These paths are active-active. For additional information, see iSCSI Session Management.

Path Failover and Virtual Machines

A path failover occurs when the active path to a LUN is changed from one path to another. Typically, the path failover occurs as a result of a SAN component failure along the current path.

When a path fails, storage I/O might pause for 30-60 seconds until your host determines that the link is unavailable and performs the failover. If you attempt to display the host, its storage devices, or its adapters, the operation might appear to stall. Virtual machines with their disks installed on the SAN can appear unresponsive. After the failover, I/O resumes normally and the virtual machines continue to run.

A Windows virtual machine might interrupt the I/O and eventually fail when failovers take too long. To avoid the failure, set the disk timeout value for the Windows virtual machine to at least 60 seconds.

Set Timeout on Windows Guest OS

To avoid disruptions during a path failover, increase the standard disk timeout value on a Windows guest operating system.

Back up the Windows registry.

This procedure explains how to change the timeout value by using the Windows registry.

1. Select **Start** > **Run**.
2. Type `regedit.exe`, and click **OK**.
3. In the left-panel hierarchy view, double-click **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Services** > **Disk**.
4. Double-click **TimeOutValue**.
5. Set the value data to 0x3c (hexadecimal) or 60 (decimal) and click **OK**.

   After you make this change, Windows waits at least 60 seconds for delayed disk operations to finish before it generates errors.
6. Reboot guest OS for the change to take effect.

Pluggable Storage Architecture and Path Management

This topic introduces the key concepts behind the ESXi storage multipathing.

Pluggable Storage Architecture (PSA)	To manage multipathing, ESXi uses a special VMkernel layer, Pluggable Storage Architecture (PSA). The PSA is an open and modular framework that coordinates various software modules responsible for multipathing operations. These modules include generic multipathing modules that VMware provides, NMP and HPP, and third-party MPPs.
Native Multipathing Plug-in (NMP)	The NMP is the VMkernel multipathing module that ESXi provides by default. The NMP associates physical paths with a specific storage device and provides a default path selection algorithm based on the array type. The NMP is extensible and manages additional submodules, called Path Selection Policies (PSPs) and Storage Array Type Policies (SATPs). PSPs and SATPs can be provided by VMware, or by a third party.
Path Selection Plug-ins (PSPs)	The PSPs are submodules of the VMware NMP. PSPs are responsible for selecting a physical path for I/O requests.
Storage Array Type Plug-ins (SATPs)	The SATPs are submodules of the VMware NMP. SATPs are responsible for array-specific operations. The SATP can determine

	the state of a particular array-specific path, perform a path activation, and detect any path errors.
Multipathing Plug-ins (MPPs)	The PSA offers a collection of VMkernel APIs that third parties can use to create their own multipathing plug-ins (MPPs). The modules provide specific load balancing and failover functionalities for a particular storage array. The MPPs can be installed on the ESXi host. They can run in addition to the VMware native modules, or as their replacement.
VMware High-Performance Plug-in (HPP)	The HPP replaces the NMP for high-speed devices, such as NVMe. The HPP can improve the performance of ultra-fast flash devices that are installed locally on your ESXi host, and is the default plug-in that claims NVMe-oF targets. To support multipathing, the HPP uses the Path Selection Schemes (PSS). A particular PSS is responsible for selecting physical paths for I/O requests. For information, see VMware High Performance Plug-In and Path Selection Schemes.
Claim Rules	The PSA uses claim rules to determine which plug-in owns the paths to a particular storage device.

Table 222: Multipathing Acronyms

Acronym	Definition
PSA	Pluggable Storage Architecture
NMP	Native Multipathing Plug-in. Generic VMware multipathing module that is used SCSI storage devices.
PSP	Path Selection Plug-in. Handles path selection for a SCSI storage device.
SATP	Storage Array Type Plug-in. Handles path failover for a given SCSI storage array.
MPP (third-party)	Multipathing Plug-in. A multipathing module developed and provided by a third party.
HPP	Native High-Performance Plug-in provided by VMware. It is used with ultra-fast local and networked flash devices, such as NVMe.
PSS	Path Selection Scheme. Handles multipathing for NVMe storage devices.

About Pluggable Storage Architecture

Pluggable Storage Architecture (PSA) is an open and modular framework that coordinates various software modules responsible for multipathing operations.

VMware provides generic native multipathing modules, called VMware NMP and VMware HPP. In addition, the PSA offers a collection of VMkernel APIs that third-party developers can use. The software developers can create their own load balancing and failover modules for a particular storage array. These third-party multipathing modules (MPPs) can be installed on the ESXi host and run in addition to the VMware native modules, or as their replacement.

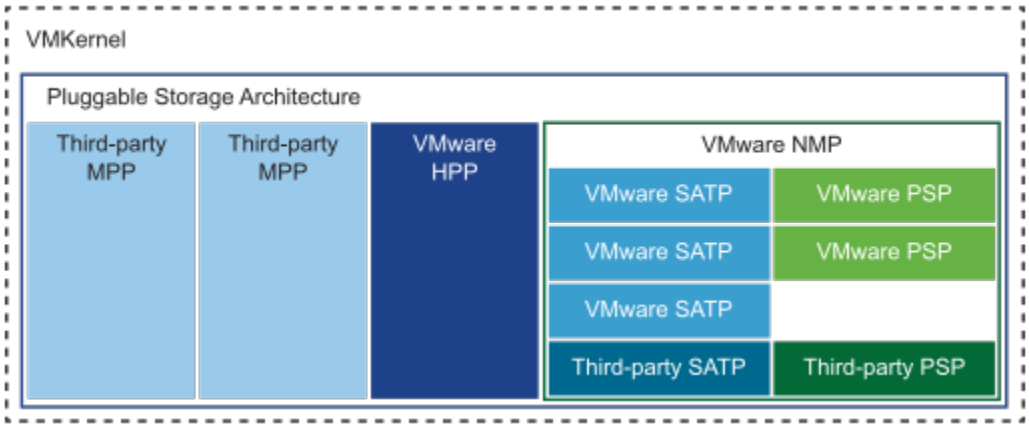
When coordinating the VMware native modules and any installed third-party MPPs, the PSA performs the following tasks:

- Loads and unloads multipathing plug-ins.
- Hides virtual machine specifics from a particular plug-in.
- Routes I/O requests for a specific logical device to the MPP managing that device.
- Handles I/O queueing to the logical devices.
- Implements logical device bandwidth sharing between virtual machines.
- Handles I/O queueing to the physical storage HBAs.

- Handles physical path discovery and removal.
- Provides logical device and physical path I/O statistics.

As the Pluggable Storage Architecture illustration shows, multiple third-party MPPs can run in parallel with the VMware NMP or HPP. When installed, the third-party MPPs can replace the behavior of the native modules. The MPPs can take control of the path failover and the load-balancing operations for the specified storage devices.

Figure 78: Pluggable Storage Architecture



VMware Native Multipathing Plug-In

By default, ESXi provides an extensible multipathing module called Native Multipathing Plug-In (NMP).

Generally, the VMware NMP supports all storage arrays listed on the VMware storage HCL and provides a default path selection algorithm based on the array type. The NMP associates a set of physical paths with a specific storage device, or LUN.

For additional multipathing operations, the NMP uses submodules, called SATPs and PSPs. The NMP delegates to the SATP the specific details of handling path failover for the device. The PSP handles path selection for the device.

Typically, the NMP performs the following operations:

- Manages physical path claiming and unclaiming.
- Registers and de-registers logical devices.
- Associates physical paths with logical devices.
- Supports path failure detection and remediation.
- Processes I/O requests to logical devices:
  - Selects an optimal physical path for the request.
  - Performs actions necessary to handle path failures and I/O command retries.
- Supports management tasks, such as reset of logical devices.

ESXi automatically installs an appropriate SATP for an array you use. You do not need to obtain or download any SATPs.

VMware NMP Flow of I/O

When a virtual machine issues an I/O request to a storage device managed by the NMP, the following process takes place.

1. The NMP calls the PSP assigned to this storage device.
2. The PSP selects an appropriate physical path on which to issue the I/O.

3. The NMP issues the I/O request on the path selected by the PSP.
4. If the I/O operation is successful, the NMP reports its completion.
5. If the I/O operation reports an error, the NMP calls the appropriate SATP.
6. The SATP interprets the I/O command errors and, when appropriate, activates the inactive paths.
7. The PSP is called to select a new path on which to issue the I/O.

Display Multipathing Modules

Use the `esxcli` command to list all multipathing modules loaded into the system. Multipathing modules manage physical paths that connect your host with storage. The modules include VMware native NMP and HPP, and any third-party MPPs.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To list multipathing modules, run the following command:

```
esxcli storage core plugin list --plugin-class=MP
```

This command typically shows the NMP and, if loaded, the HPP and the MASK_PATH module. If any third-party MPPs have been loaded, they are listed as well.

```
Plugin name  Plugin class
-----------  ------------
NMP          MP
```

For more information about the command, see the *ESXCLI Concepts and Examples* and *ESXCLI Reference* documentation.

Display NMP Storage Devices

Use the `esxcli` command to list all storage devices controlled by the VMware NMP and display SATP and PSP information associated with each device.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To list all storage devices, run the following command:

```
esxcli storage nmp device list
```

Use the `--device | -d=`*`device_ID`* parameter to filter the output of this command to show a single device.

Displaying NMP Storage Devices

```
# esxcli storage nmp device list
mpx.vmhba1:C0:T2:L0
   Device Display Name: Local VMware Disk (mpx.vmhba1:C0:T2:L0)
   Storage Array Type: VMW_SATP_LOCAL
   Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device configuration.
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba1:C0:T2:L0;current=vmhba1:C0:T2:L0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba1:C0:T2:L0
   Is USB: false

......

eui.6238666462643332
   Device Display Name: SCST_BIO iSCSI Disk (eui.6238666462643332)
   Storage Array Type: VMW_SATP_DEFAULT_AA
```

```
Storage Array Type Device Config: {action_OnRetryErrors=off}
Path Selection Policy: VMW_PSP_FIXED
Path Selection Policy Device Config: {preferred=vmhba65:C0:T0:L0;current=vmhba65:C0:T0:L0}
Path Selection Policy Device Custom Config:
Working Paths: vmhba65:C0:T0:L0
Is USB: false
```

For more information about the command, see the *ESXCLI Concepts and Examples* and *ESXCLI Reference* documentation.

Path Selection Plug-Ins and Policies

VMware Path Selection Plug-ins (PSPs) are responsible for selecting a physical path for I/O requests.

The plug-ins are submodules of the VMware NMP. The NMP assigns a default PSP for each logical device based on the device type. You can override the default PSP. For more information, see Change the Path Selection Policy.

Each PSP enables and enforces a corresponding path selection policy.

VMW_PSP_MRU - Most Recently Used (VMware)	The Most Recently Used (VMware) policy is enforced by VMW_PSP_MRU. It selects the first working path discovered at system boot time. When the path becomes unavailable, the host selects an alternative path. The host does not revert to the original path when that path becomes available. The Most Recently Used policy does not use the preferred path setting. This policy is default for most active-passive storage devices. The VMW_PSP_MRU supports path ranking. To set ranks to individual paths, use the `esxcli storage nmp psp generic pathconfig set` command. For details, see the VMware knowledge base article at http://kb.vmware.com/kb/2003468 and the *ESXCLI Reference* documentation.
VMW_PSP_FIXED - Fixed (VMware)	This Fixed (VMware) policy is implemented by VMW_PSP_FIXED. The policy uses the designated preferred path. If the preferred path is not assigned, the policy selects the first working path discovered at system boot time. If the preferred path becomes unavailable, the host selects an alternative available path. The host returns to the previously defined preferred path when it becomes available again. Fixed is the default policy for most active-active storage devices.
VMW_PSP_RR - Round Robin (VMware)	VMW_PSP_RR enables the Round Robin (VMware) policy. Round Robin is the default policy for many arrays. It uses an automatic path selection algorithm rotating through the configured paths. Both active-active and active-passive arrays use the policy to implement load balancing across paths for different LUNs. With active-passive arrays, the policy uses active paths. With active-active arrays, the policy uses available paths. The latency mechanism that can be activated for the policy makes it more adaptive. To achieve better load balancing results, the mechanism dynamically selects an optimal path by considering the following path characteristics: • I/O bandwidth • Path latency To change the default parameters for the adaptive latency Round Robin policy or to deactivate the latency mechanism, see the Change Default Parameters for Latency Round Robin.

To set other configurable parameters for VMW_PSP_RR, use the `esxcli storage nmp psp roundrobin` command. For details, see the *ESXCLI Reference* documentation.

VMware SATPs

Storage Array Type Plug-ins (SATPs) are responsible for array-specific operations. The SATPs are submodules of the VMware NMP.

ESXi offers an SATP for every type of array that VMware supports. ESXi also provides default SATPs that support non-specific active-active, active-passive, ALUA, and local devices.

Each SATP accommodates special characteristics of a certain class of storage arrays. The SATP can perform the array-specific operations required to detect path state and to activate an inactive path. As a result, the NMP module itself can work with multiple storage arrays without having to be aware of the storage device specifics.

Generally, the NMP determines which SATP to use for a specific storage device and associates the SATP with the physical paths for that storage device. The SATP implements the tasks that include the following:

- Monitors the health of each physical path.
- Reports changes in the state of each physical path.
- Performs array-specific actions necessary for storage fail-over. For example, for active-passive devices, it can activate passive paths.

ESXi includes several generic SATP modules for storage arrays.

VMW_SATP_LOCAL	SATP for local direct-attached devices. As of vSphere 6.5 Update 2 release, VMW_SATP_LOCAL provides multipathing support for the local devices, except the devices in 4K native format. To claim multiple paths to the local devices, you are no longer required to use other SATPs as you were in the earlier vSphere releases. VMW_SATP_LOCAL supports the VMW_PSP_MRU and VMW_PSP_FIXED path selection plug-ins, but does not support VMW_PSP_RR.
VMW_SATP_DEFAULT_AA	Generic SATP for active-active arrays.
VMW_SATP_DEFAULT_AP	Generic SATP for active-passive arrays.
VMW_SATP_ALUA	SATP for ALUA-compliant arrays.

For more information, see the *VMware Compatibility Guide* and the *ESXCLI Reference* documentation.

Display SATPs for the Host

Use the `esxcli` command to list VMware NMP SATPs loaded into the system. Display information about the SATPs.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To list VMware SATPs, run the following command:

```
esxcli storage nmp satp list
```

For each SATP, the output displays information that shows the type of storage array or system the SATP supports. The output also shows the default PSP for any LUNs that use this SATP. `Placeholder (plugin not loaded)` in the Description column indicates that the SATP is not loaded.

Displaying SATPs for the Host

```
# esxcli storage nmp satp list
Name                 Default PSP    Description
VMW_SATP_MSA         VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_ALUA        VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AP  VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_SVC         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_EQL         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_INV         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_EVA         VMW_PSP_FIXED  Placeholder (plugin not loaded)
VMW_SATP_ALUA_CX     VMW_PSP_RR     Placeholder (plugin not loaded)
VMW_SATP_SYMM        VMW_PSP_RR     Placeholder (plugin not loaded)
VMW_SATP_CX          VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_LSI         VMW_PSP_MRU    Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AA  VMW_PSP_FIXED  Supports non-specific active/active arrays
VMW_SATP_LOCAL       VMW_PSP_FIXED  Supports direct attached devices
```

For more information about the command, see the *ESXCLI Concepts and Examples* and *ESXCLI Reference* documentation.

VMware High Performance Plug-In and Path Selection Schemes

VMware provides the High-Performance Plug-in (HPP) to improve the performance of storage devices on your ESXi host.

The HPP replaces the NMP for high-speed devices, such as NVMe. The HPP is the default plug-in that claims NVMe-oF targets. Within ESXi, the NVMe-oF targets are emulated and presented to users as SCSI targets. The HPP supports only active/active and implicit ALUA targets.

In vSphere version 7.0 Update 1 and earlier, NMP remains the default plug-in for local NVMe devices, but you can replace it with HPP. Starting from vSphere 7.0 Update 2, HPP becomes the default plug-in for local NVMe and SCSI devices, but you can replace it with NMP.

HPP Support	vSphere 7.0 Update 1	vSphere 7.0 Update 2 and Update 3
Storage devices	Local NVMe PCIe Shared NVMe-oF (active/active and implicit ALUA targets only)	Local NVMe and SCSI Shared NVMe-oF (active/active and implicit ALUA targets only)
Multipathing	Yes	Yes
Second-level plug-ins	No Path Selection Schemes (PSS)	No
SCSI-3 persistent reservations	No	No
4Kn devices with software emulation	No	Yes

Path Selection Schemes

To support multipathing, the HPP uses the Path Selection Schemes (PSS) when selecting physical paths for I/O requests.

You can use the vSphere Client or the `esxcli` command to change the default path selection mechanism.

For information about configuring the path mechanisms in the vSphere Client, see Change the Path Selection Policy. To configure with the `esxcli` command, see ESXi esxcli HPP Commands.

ESXi supports the following path selection mechanisms.

FIXED	With this scheme, a designated preferred path is used for I/O requests. If the preferred path is not assigned, the host selects the first working path discovered at the boot time. If the preferred path becomes unavailable, the host selects an alternative available path. The host returns to the previously defined preferred path when it becomes available again. When you configure **FIXED** as a path selection mechanism, select the preferred path.
LB-RR (Load Balance - Round Robin)	This is the default scheme for the devices claimed by HPP. After transferring a specified number of bytes or I/Os on a current path, the scheme selects the path using the round robin algorithm. To configure the **LB-RR** path selection mechanism, specify the following properties: • **IOPS** indicates the I/O count on the path to be used as criteria to switch a path for the device. • **Bytes** indicates the byte count on the path to be used as criteria to switch a path for the device.
LB-IOPS (Load Balance - IOPs)	After transferring a specified number of I/Os on a current path, default is 1000, the system selects an optimal path that has the least number of outstanding I/Os. When configuring this mechanism, specify the **IOPS** parameter to indicate the I/O count on the path to be used as criteria to switch a path for the device.
LB-BYTES (Load Balance - Bytes)	After transferring a specified number of bytes on a current path, default is 10 MB, the system selects an optimal path that has the least number of outstanding bytes. To configure this mechanism, use the **Bytes** parameter to indicate the byte count on the path to be used as criteria to switch a path for the device.
Load Balance - Latency (LB-Latency)	To achieve better load balancing results, the mechanism dynamically selects an optimal path by considering the following path characteristics: • **Latency evaluation time** parameter indicates at what time interval, in milliseconds, the latency of paths must be evaluated. • **Sampling I/Os per path** parameter controls how many sample I/Os must be issued on each path to calculate latency of the path.

HPP Best Practices

To achieve the fastest throughput from a high-speed storage device, follow these recommendations.

- Use the vSphere version that supports the HPP.
- Use the HPP for local NVMe and SCSI devices, and NVMe-oF devices.
- If you use NVMe over Fibre Channel devices, follow general recommendations for Fibre Channel storage. See Using ESXi with Fibre Channel SAN.
- If you use NVMe-oF, do not mix transport types to access the same namespace.
- When using NVMe-oF namespaces, make sure that active paths are presented to the host. The namespaces cannot be registered until the active path is discovered.

- When you configure your VMs, you can use VMware Paravirtual controllers or add NVMe controllers. Both types have their advantages and disadvantages. To check which works best for your environment, see SCSI, SATA, and NVMe Storage Controller Conditions, Limitations, and Compatibility in the *vSphere Virtual Machine Administration* documentation.
- Set the latency sensitive threshold.
- If a single VM drives a significant share of the device's I/O workload, consider spreading the I/O across multiple virtual disks. Attach the disks to separate virtual controllers in the VM.
  Otherwise, I/O throughput might be limited due to saturation of the CPU core responsible for processing I/Os on a particular virtual storage controller.

For information about device identifiers for NVMe devices that support only NGUID ID format, see NVMe Devices with NGUID Device Identifiers.

Enable the High-Performance Plug-In and the Path Selection Schemes

The high-performance plug-in (HPP) is the default plug-in that claims local NVMe and SCSI devices, and NVMe-oF targets. If necessary, you can replace it with NMP. In vSphere version 7.0 Update 1 and earlier, NMP remains the default plug-in for local NVMe and SCSI devices, but you can replace it with HPP.

Set up your VMware NVMe storage environment. For more information, see About VMware NVMe Storage.

Use the `esxcli storage core claimrule add` command to enable the HPP or NMP on your ESXi host.

To run the `esxcli storage core claimrule add`, you can use the ESXi Shell or vSphere CLI. For more information, see *Getting Started with ESXCLI* and *ESXCLI Reference*.

Examples in this topic demonstrate how to enable HPP and set up the path selection schemes (PSS).

Note: Enabling the HPP is not supported on PXE booted ESXi hosts.

1. Create an HPP claim rule by running the `esxcli storage core claimrule add` command.
   Use one of the following methods to add the claim rule.

Method	Description
Based on the NVMe controller model	`esxcli storage core claimrule add --type vendor --nvme-controller-model` For example, `esxcli storage core claimrule add --rule 429 --type vendor --nvme-controller-model "ABCD*" --plugin HPP`
Based on the PCI vendor ID and subvendor ID	`esxcli storage core claimrule add --type vendor --pci-vendor-id --pci-sub-vendor-id` For example, `esxcli storage core claimrule add --rule 429 --type vendor --pci-vendor-id 8086 --pci-sub-vendor-id 8086 --plugin HPP`.

2. Configure the PSS.
   Use one of the following methods.

Method	Description
Set the PSS based on the device ID	`esxcli storage hpp device set` For example, `esxcli storage hpp device set --device=`*`device`* `--pss=FIXED --path=preferred path`
Set the PSS based on the vendor/model	Use the `--config-string` option with the `esxcli storage core claimrule add` command.

Method	Description
	For example, `esxcli storage core claimrule add -r 914 -t vendor -V vendor -M model -P HPP --config-string "pss=LB-Latency,latency-eval-time=40000"`

3. Reboot your host for your changes to take effect.

Set Latency Sensitive Threshold

When you use the HPP for your storage devices, set the latency sensitive threshold for the device, so that I/O can avoid the I/O scheduler.

By default, ESXi passes every I/O through the I/O scheduler. However, using the scheduler might create internal queuing, which is not efficient with the high-speed storage devices.

You can configure the latency sensitive threshold and enable the direct submission mechanism that helps I/O to bypass the scheduler. With this mechanism enabled, the I/O passes directly from PSA through the HPP to the device driver.

For the direct submission to work properly, the observed average I/O latency must be lower than the latency threshold you specify. If the I/O latency exceeds the latency threshold, the system stops the direct submission and temporarily reverts to using the I/O scheduler. The direct submission is resumed when the average I/O latency drops below the latency threshold again.

You can set the latency threshold for a family of devices claimed by HPP. Set the latency threshold using the vendor and model pair, the controller model, or PCIe vendor ID and sub vendor ID pair.

1. Set the latency sensitive threshold for the device by running the following command:

   `esxcli storage core device latencythreshold set -t value in milliseconds`

   Use one of the following options.

Option	Example
Vendor/model	Set the latency sensitive threshold parameter for all devices with the indicated vendor and model: `esxcli storage core device latencythreshold set -v 'vendor1' -m 'model1' -t 10`
NVMe controller model	Set the latency sensitive threshold for all NVMe devices with the indicated controller model: `esxcli storage core device latencythreshold set -c 'controller_model1' -t 10`
PCIe vendor/subvendor ID	Set the latency sensitive threshold for devices with 0x8086 as PCIe vendor ID and 0x8086 as PCIe sub vendor ID. `esxcli storage core device latencythreshold set -p '8086' -s '8086' -t 10`

2. Verify that the latency threshold is set:

   ```
   esxcli storage core device latencythreshold list
   ```

   ```
   Device                Latency Sensitive Threshold
   --------------------  ---------------------------
   naa.55cd2e404c1728aa               0 milliseconds
   naa.500056b34036cdfd               0 milliseconds
   naa.55cd2e404c172bd6              50 milliseconds
   ```

3. Monitor the status of the latency sensitive threshold. Check VMkernel logs for the following entries:
   - `Latency Sensitive Gatekeeper turned on for device device. Threshold of XX msec is larger than max completion time of YYY msec`
   - `Latency Sensitive Gatekeeper turned off for device device. Threshold of XX msec is exceeded by command completed in YYY msec`

ESXi esxcli HPP Commands

You can use the ESXi Shell or vSphere CLI commands to configure and monitor the high-performance plug-in.

See *Getting Started with ESXCLI* for an introduction, and *ESXCLI Reference* for details of the `esxcli` command use.

Command	Description	Options
`esxcli storage hpp path list`	List the paths currently claimed by the high-performance plug-in.	`-d|--device=device` Display information for a specific device. `-p|--path=path` Limit the output to a specific path.
`esxcli storage hpp device list`	List the devices currently controlled by the high-performance plug-in.	`-d|--device=device` Show a specific device.
`esxcli storage hpp device set`	Configure settings for an HPP device.	`-B|--bytes=long` Maximum bytes on the path, after which the path is switched. `--cfg-file` Update the configuration file and runtime with the new setting. If the device is claimed by another PSS, ignore any errors when applying to runtime configuration. `-d|--device=device` The HPP device upon which to operate. Use any of the UIDs that the device reports. Required. `-I|--iops=long` Maximum IOPS on the path, after which the path is switched. `-T|--latency-eval-time=long` Control at what interval, in ms, the latency of paths must be evaluated. `-L|--mark-device-local=bool` Set HPP to treat the device as local or not. `-M|--mark-device-ssd=bool` Specify whether or not the HPP treats the device as an SSD. `-p|--path=str` The path to set as the preferred path for the device. `-P|--pss=pss_name` The path selection scheme to assign to the device. If you do not specify the value, the system selects the default. For the description of path selection schemes, see VMware High Performance Plug-In and Path Selection Schemes. Options include: • `FIXED` Use the `-p|--path=str` suboption to set the preferred path.

Command	Description	Options
		• `LB-Bytes` Use the `-B|--bytes=`*`long`* suboption to specify the input. • `LB-IOPs` Use the `-I|--iops=`*`long`* suboption to specify the input. • `LB-Latency` Suboptions include: `-T|--latency-eval-time=`*`long`* `-S|--sampling-ios-per-path=`*`long`* • `LB-RR` Default Suboptions include: `-B|--bytes=`*`long`* `-I|--iops=`*`long`* `-S|--sampling-ios-per-path=`*`long`* Control how many sample I/Os must be issued on each path to calculate latency of the path. `-U|--use-ano=`*`bool`* Set the option to `true` to include non-optimized paths in the set of active paths used to issue I/Os on this device. Otherwise, set the option to `false`.
`esxcli storage hpp device usermarkedssd list`	List the devices that were marked or unmarked as SSD by user.	`-d|--device=`*`device`* Limit the output to a specific device.

Viewing and Managing Paths

When you start your ESXi host or rescan your storage adapter, the host discovers all physical paths to storage devices available to the host. Based on a set of claim rules, the host determines which multipathing module, the NMP, HPP, or an MPP, owns the paths to a particular device.

The module that owns the device becomes responsible for managing the multipathing support for the device. By default, the host performs a periodic path evaluation every five minutes and assigns unclaimed paths to the appropriate module.

For the paths managed by the NMP module, a second set of claim rules is used. These rules assign an SATP and PSP modules to each storage device and determine which Storage Array Type Policy and Path Selection Policy to apply.

Use the vSphere Client to view the Storage Array Type Policy and Path Selection Policy assigned to a specific storage device. You can also check the status of all available paths for this storage device. If needed, you can change the default Path Selection Policy using the client.

To change the default multipathing module or SATP, modify claim rules using the vSphere CLI.

You can find some information about modifying claim rules in Using Claim Rules.

View Storage Device Paths

View which multipathing policies the host uses for a specific storage device and the status of all available paths for this storage device.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices**.
4. Select the storage device whose paths you want to view.
5. Click the **Properties** tab and review the module that owns the device, for example NMP or HPP.

   Under Multipathing Policies, you can also see the Path Selection Policy and, if applicable, the Storage Array Type Policy assigned to the device.
6. Click the **Paths** tab to review all paths available for the storage device and the status of each path. The following path status information can appear:

Status	Description
Active (I/O)	Working path or multiple paths that currently transfer data.
Standby	Paths that are inactive. If the active path fails, they can become operational and start transferring I/O.
Disabled	Paths that are disabled by the administrator.
Dead	Paths that are no longer available for processing I/O. A physical medium failure or array misconfiguration can cause this status.

   If you are using the **Fixed** path policy, you can see which path is the preferred path. The preferred path is marked with an asterisk (*) in the Preferred column.

View Datastore Paths

Review the paths that connect to storage devices backing your VMFS datastores.

1. In the vSphere Client, navigate to the datastore.
2. Click the **Configure** tab.
3. Click **Connectivity and Multipathing**.
4. Select a host to view multipathing details for its devices.
5. Under Multipathing Policies, review the module that owns the device, such as NMP. You can also see the Path Selection Policy and Storage Array Type Policy assigned to the device.

   For example, you might see the following:

Path Selection Policy	Preferred Path
Storage Array Type Policy	VMW_SATP_LOCAL
Owner Plugin	NMP

6. Under Paths, review the device paths and the status of each path. The following path status information can appear:

Status	Description
Active (I/O)	Working path or multiple paths that currently transfer data.
Standby	Paths that are inactive. If the active path fails, they can become operational and start transferring I/O.
Disabled	Paths that are disabled by the administrator.

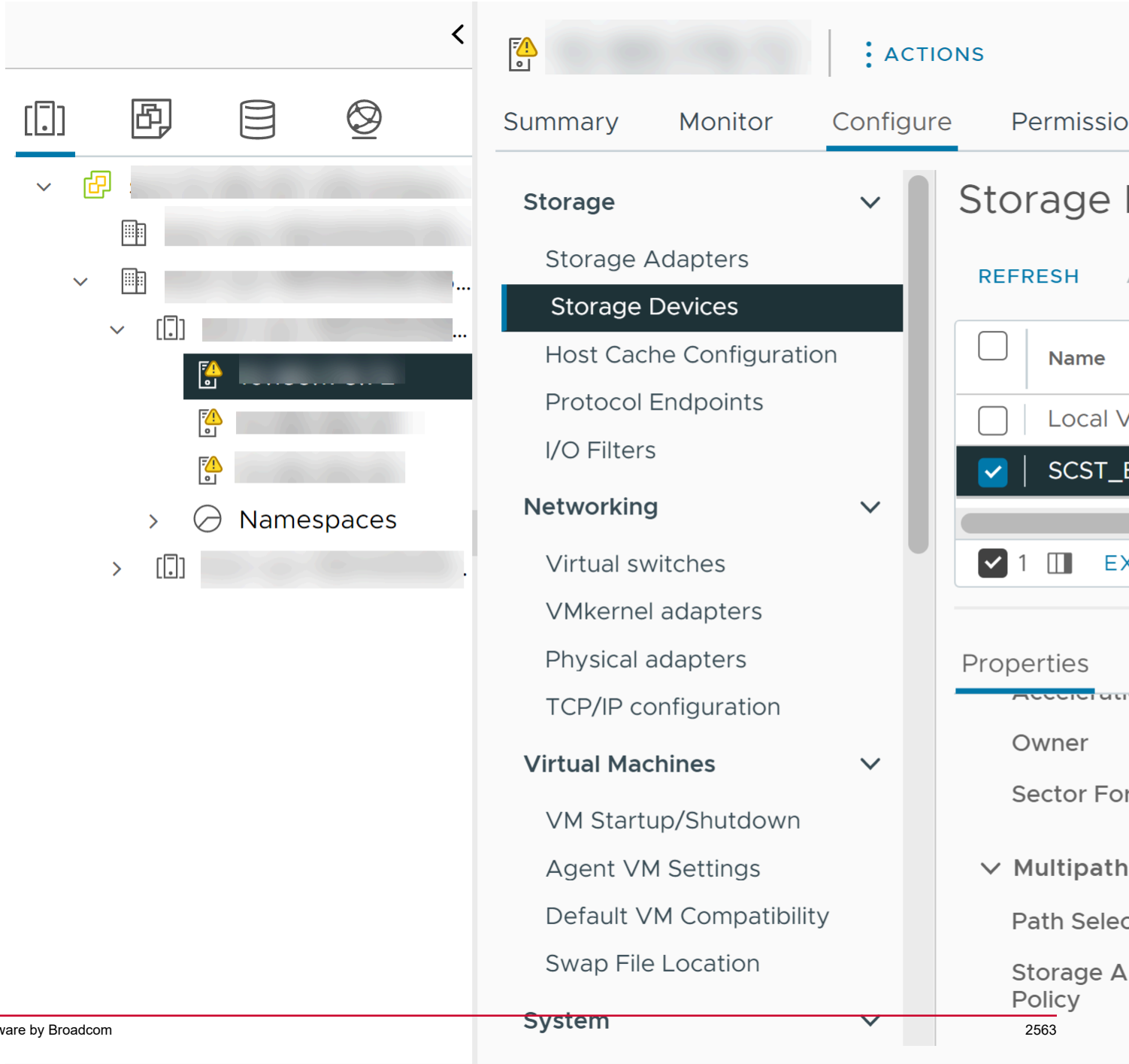
Status	Description
Dead	Paths that are no longer available for processing I/O. A physical medium failure or array misconfiguration can cause this status.

If you are using the **Fixed** path policy, you can see which path is the preferred path. The preferred path is marked with an asterisk (*) in the Preferred column.

Change the Path Selection Policy

Generally, you do not need to change the default multipathing settings that your ESXi host uses for a specific storage device. If you want to make any changes, you can use the **Edit Multipathing Policies** dialog box to modify the path selection policy. You can also use this dialog box to change multipathing for SCSI-based protocol endpoints.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Storage Devices** or **Protocol Endpoints**.
4. Select the item whose paths you want to change and click the **Properties** tab.
5. Under Multipathing Policies, select **Edit Multipathing** from the **Actions** menu.



6. Select a path policy and configure its settings. Your options change depending on the type of a storage device you use.
   - For information about path policies for SCSI devices, see Path Selection Plug-Ins and Policies.
   - For information about path mechanisms for NVMe devices, see VMware High Performance Plug-In and Path Selection Schemes.
7. To save your settings and exit the dialog box, click **OK**.

Change Default Parameters for Latency Round Robin

On the ESXi host, you can activate the latency mechanism for the Round Robin path selection policy. The mechanism considers I/O bandwidth and path latency to select an optimal path for I/O. When using the latency mechanism, the Round Robin policy can dynamically select the optimal path and achieve better load balancing results.

Set the path selection policy to Round Robin. See Change the Path Selection Policy.

When latency is activated, usage of paths for the I/Os depends on the workload. When a large number of paths is available, but the workload is not high enough, the system might not use some paths for I/Os.

You use the `esxcli` command to change the default parameters of the latency mechanism or deactivate the mechanism.

1. Configure the latency mechanism by using the following command.

   ```
   esxcli storage nmp psp roundrobin deviceconfig set --type=latency --device=device ID
   ```

   The command takes the following parameters:

Parameter	Description
-S|--num-sampling-cycles=*sampling value*	When `--type` is set to `latency`, this parameter controls how many I/Os to use to calculate the average latency of each path. The default value of this parameter is 16.
-T|--latency-eval-time=*time in ms*	When `--type` is set to `latency`, this parameter controls the frequency at which the latency of paths is updated. Default is 3 minutes.

2. Verify whether the latency Round Robin and its parameters are configured correctly.

   ```
   esxcli storage nmp psp roundrobin deviceconfig get --device=device ID
   ```

   or

   ```
   esxcli storage nmp device list --device=device ID
   ```

   The following sample output shows the path's configuration:

   ```
   Path Selection Policy: VMW_PSP_RR
   Path Selection Policy Device Config: {policy=latency,latencyEvalTime=180000,samplingCycles=16,curSampling-
   Cycle=16,useANO=0; CurrentPath=vmhba1:C0:T0:L0: NumIOsPending=0,latency=0}
   ```

To deactivate the latency mechanism, in the Advanced System Settings for your host, change the `Misc.EnablePSPLatencyPolicy` parameter to 0.

Disable Storage Paths

You can temporarily disable paths for maintenance or other reasons.

You disable a path using the Paths panel. You have several ways to access the Paths panel, from a datastore, a storage device, an adapter, or a Virtual Volumes Protocol Endpoint view.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click one of the following items:
   - **Storage Adapters**
   - **Storage Devices**
   - **Protocol Endpoints**
4. In the right pane, select the item whose paths you want to disable, an adapter, storage device, or Protocol Endpoint, and click the **Paths** tab.
5. Select the path to disable and click **Disable**.

   The path's status changes to Disabled.

Using Claim Rules

Claim rules determine which multipathing module owns the paths to a particular storage device. They also define the type of multipathing support that the host provides to the device.

The rules fall into these categories:

Core Claim Rules	These claim rules determine which multipathing module, the NMP, HPP, or a third-party MPP, claims the specific device.
SATP Claim Rules	Depending on the device type, these rules assign a particular SATP submodule that provides vendor-specific multipathing management to the device.

You can use the `esxcli` commands to add or change the core and SATP claim rules. Typically, you add the claim rules to load a third-party MPP or to hide a LUN from your host. Changing claim rules might be necessary when default settings for a specific device are not sufficient.

For more information about commands available to manage PSA claim rules, see the *Getting Started with ESXCLI*.

For a list of storage arrays and corresponding SATPs and PSPs, see the Storage/SAN section of the *vSphere Compatibility Guide*.

Multipathing Considerations

Specific considerations apply when you manage storage multipathing plug-ins and claim rules.

The following considerations help you with multipathing:

- If no SATP is assigned to the device by the claim rules, the default SATP for iSCSI or FC devices is VMW_SATP_DEFAULT_AA. The default PSP is VMW_PSP_FIXED.
- When the system searches the SATP rules to locate a SATP for a given device, it searches the driver rules first. If there is no match, the vendor/model rules are searched, and finally the transport rules are searched. If no match occurs, NMP selects a default SATP for the device.
- If VMW_SATP_ALUA is assigned to a specific storage device, but the device is not ALUA-aware, no claim rule match occurs for this device. The device is claimed by the default SATP based on the device's transport type.

- The default PSP for all devices claimed by VMW_SATP_ALUA is VMW_PSP_MRU. The VMW_PSP_MRU selects an active/optimized path as reported by the VMW_SATP_ALUA, or an active/unoptimized path if there is no active/optimized path. This path is used until a better path is available (MRU). For example, if the VMW_PSP_MRU is currently using an active/unoptimized path and an active/optimized path becomes available, the VMW_PSP_MRU will switch the current path to the active/optimized one.
- While VMW_PSP_MRU is typically selected for ALUA arrays by default, certain ALUA storage arrays need to use VMW_PSP_FIXED. To check whether your storage array requires VMW_PSP_FIXED, see the *VMware Compatibility Guide* or contact your storage vendor. When using VMW_PSP_FIXED with ALUA arrays, unless you explicitly specify a preferred path, the ESXi host selects the most optimal working path and designates it as the default preferred path. If the host selected path becomes unavailable, the host selects an alternative available path. However, if you explicitly designate the preferred path, it will remain preferred no matter what its status is.
- By default, the PSA claim rule 101 masks Dell array pseudo devices. Do not delete this rule, unless you want to unmask these devices.

List Multipathing Claim Rules for the Host

Use the `esxcli` command to list available multipathing claim rules.

Claim rules indicate whether the NMP, HPP, or a third-party MPP manages a given physical path. Each claim rule identifies a set of paths based on the following parameters:

- Vendor/model strings
- Transportation, such as SATA, IDE, Fibre Channel
- Adapter, target, or LUN location
- Device driver, for example, Mega-RAID

List the multipathing claim rules by running the `esxcli storage core claimrule list --claimrule-class=MP` command.

If you do not use the `claimrule-class` option, the MP rule class is implied.

Sample Output of the esxcli storage core claimrule list Command

```
Rule Class  Rule   Class    Type       Plugin     Matches
MP           10    runtime  vendor     HPP        vendor=NVMe model=*
MP           10    file     vendor     HPP        vendor=NVMe model=*
MP           50    runtime  transport  NMP        transport=usb
MP           51    runtime  transport  NMP        transport=sata
MP           52    runtime  transport  NMP        transport=ide
MP           53    runtime  transport  NMP        transport=block
MP           54    runtime  transport  NMP        transport=unknown
MP          101    runtime  vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          101    file     vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          200    runtime  vendor     MPP_1      vendor=NewVend model=*
MP          200    file     vendor     MPP_1      vendor=NewVend model=*
MP          201    runtime  location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          201    file     location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          202    runtime  driver     MPP_3      driver=megaraid
MP          202    file     driver     MPP_3      driver=megaraid
MP          65535  runtime  vendor     NMP        vendor=* model=*
```

This example indicates the following:

- The NMP claims all paths connected to storage devices that use the USB, SATA, IDE, and Block SCSI transportation.

- The rules for HPP, MPP_1, MPP_2, and MPP_3 have been added, so that the modules can claim specified devices. For example, the HPP claims all devices with vendor NVMe. All devices handled by the inbox nvme driver are claimed regardless of the actual vendor. The MPP_1 module claims all paths connected to any model of the NewVend storage array.
- You can use the MASK_PATH module to hide unused devices from your host. By default, the PSA claim rule 101 masks Dell array pseudo devices with a vendor string `DELL` and a model string `Universal Xport`.
- The Rule Class column in the output describes the category of a claim rule. It can be MP (multipathing plug-in), Filter, or VAAI.
- The Class column shows which rules are defined and which are loaded. The `file` parameter in the Class column indicates that the rule is defined. The `runtime` parameter indicates that the rule has been loaded into your system. For a user-defined claim rule to be active, two lines with the same rule number must exist, one line for the rule with the `file` parameter and another line with `runtime`. Several default system-defined claim rules have only one line with the Class of `runtime`. You cannot modify these rules.
- The default rule 65535 assigns all unclaimed paths to the NMP. Do not delete this rule.

Add Multipathing Claim Rules

Use the `esxcli` commands to add a multipathing PSA claim rule to the set of claim rules on the system. For the new claim rule to be active, you first define the rule and then load it into your system.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Examples when you add a PSA claim rule include the following:

- You load a new third-party MPP and must define the paths that this module claims.
- You must enable the native HPP.

Warning: You cannot create rules where two different plug-ins claim paths to the same device. Your attempts to create these claim rules fail with a warning in `vmkernel.log`.

1. To define a new claim rule, use the following command:

   ```
   esxcli storage core claimrule add
   ```

   The command takes the following options:

Option	Description
-A|--adapter=<adapter>	Adapter of the paths to use. Valid only if `--type` is `location` .
-u|--autoassign	Adds a claim rule based on its characteristics. The rule number is not required.
-C|--channel=<channel>	Channel of the paths to use. Valid only if `--type` is `location` .
-c|--claimrule-class=<cl>	Claim rule class to use in this operation. You can specify `MP` (default), `Filter` , or `VAAI` . To configure hardware acceleration for a new array, add two claim rules, one for the VAAI filter and another for the VAAI plug-in. See Add Hardware Acceleration Claim Rules for detailed instructions.
-d|--device=<device_uid>	UID of the device. Valid only when `--type` is `device` .
-D|--driver=<driver>	Driver for the HBA of the paths to use. Valid only if `--type` is `driver` .
-f|--force	Force claim rules to ignore validity checks and install the rule anyway.

Option	Description
--force-reserved	Override protection of reserved rule ID ranges. Reserved claim rules are the rules with an ID below 100. You can use them to reassign local devices to specific plug-ins, for example, the NVMe device to HPP.
--if-unset=<str>	Run this command if this advanced user variable is not set to 1.
-i|--iqn=<iscsi_name>	iSCSI Qualified Name for the target. Valid only when `--type` is `target`.
-L|--lun=<lun_id>	LUN of the paths. Valid only if `--type` is `location`. LUN ID must not be higher than the value of the advanced configuration option /Disk/MaxLUN.
-M|--model=<model>	Model of the paths to use. Valid only if `--type` is `vendor`. Valid values are values of the Model string from the SCSI inquiry string. Run `vicfg-scsidevs <conn_options> -l` on each device to see model string values.
-P|--plugin=<plugin>	PSA plug-in to use. The values are `NMP`, `MASK_PATH`, or `HPP`. Third parties can also provide their own PSA plug-ins. Required.
-r|--rule=<rule_ID>	Rule ID to use. The rule ID indicates the order in which the claim rule is to be evaluated. User-defined claim rules are evaluated in numeric order starting with 101. You can run `esxcli storage core claimrule list` to determine which rule IDs are available.
-T|--target=<target>	Target of the paths to use. Valid only if `--type` is `location`.
-R|--transport=<transport>	Transport of the paths to use. Valid only if `--type` is `transport`. The following values are supported. • `block` — block storage • `fc` — Fibre Channel • `iscsivendor` — iSCSI • `iscsi` — not currently used • `ide` — IDE storage • `sas` — SAS storage • `sata` — SATA storage • `usb` — USB storage • `parallel` — parallel • `fcoe` — FCoE • `unknown`
-t|--type=<type>	Type of matching to use for the operation. Valid values are the following. Required. • `vendor` • `location` • `driver` • `transport` • `device` • `target`
-V|--vendor=<vendor>	Vendor of the paths to use. Valid only if `--type` is `vendor`.

Option	Description
	Valid values are values of the vendor string from the SCSI inquiry string. Run `vicfg-scsidevs <conn_options> -l` on each device to see vendor string values.
--wwnn=<wwnn>	World-Wide Node Number for the target.
--wwpn=<wwpn>	World-Wide Port Number for the target.
-a|--xcopy-use-array-values	Use the array reported values to construct the XCOPY command to be sent to the storage array. This applies to VAAI claim rules only.
-s|--xcopy-use-multi-segs	Use multiple segments when issuing an XCOPY request. Valid only if `--xcopy-use-array-values` is specified.
-m|--xcopy-max-transfer-size	Maximum data transfer size in MB when you use a transfer size different than array reported. Valid only if `--xcopy-use-array-values` is specified.
-k|--xcopy-max-transfer-size-kib	Maximum transfer size in KiB for the XCOPY commands when you use a transfer size different than array reported. Valid only if `--xcopy-use-array-values` is specified.

2. To load the new claim rule into your system, use the following command:

   `esxcli storage core claimrule load`

   This command loads all newly created multipathing claim rules from the `esx.conf` configuration file into the VMkernel. The command has no options.

3. To apply claim rules that are loaded, use the following command:

   `esxcli storage core claimrule run`

   The command takes the following options:

Option	Description
-A|--adapter=<adapter>	If `--type` is `location`, name of the HBA for the paths to run the claim rules on. To run claim rules on paths from all adapters, omit this option.
-C|--channel=<channel>	If `--type` is `location` , value of the SCSI channel number for the paths to run the claim rules on. To run claim rules on paths with any channel number, omit this option.
-c|--claimrule-class=<cl>	Claim rule class to use in this operation.
-d|--device=<device_uid>	UID of the device.
-L|--lun=<lun_id>	If `--type` is `location` , value of the SCSI LUN for the paths to run claim rules on. To run claim rules on paths with any LUN, omit this option.
-p|--path=<path_uid>	If `--type` is `path` , this option indicates the unique path identifier (UID) or the runtime name of a path to run claim rules on.
-T|--target=<target>	If `--type` is `location` , value of the SCSI target number for the paths to run claim rules on. To run claim rules on paths with any target number, omit this option.
-t|--type=<location|path|all>	Type of claim to perform. By default, uses `all` , which means claim rules run without restriction to specific paths or SCSI addresses. Valid values are `location` , `path` , and `all` .
-w|--wait	You can use this option only if you also use `--type all` .

Option	Description
	If the option is included, the claim waits for paths to settle before running the claim operation. In that case, the system does not start the claiming process until it is likely that all paths on the system have appeared before starting the claim process. After the claiming process has started, the command does not return until device registration has completed. If you add or remove paths during the claiming or the discovery process, this option might not work correctly.

Defining Multipathing Claim Rules

In the following example, you add and load rule # 500. The rule claims all paths with the NewMod model string and the NewVend vendor string for the NMP plug-in.

```
# esxcli storage core claimrule add -r 500 -t vendor -V NewVend -M NewMod -P NMP
# esxcli storage core claimrule load
```

After you run the `esxcli storage core claimrule list` command, you can see the new claim rule appearing on the list.

The following output indicates that the claim rule 500 has been loaded into the system and is active.

```
Rule Class  Rule   Class    Type       Plugin     Matches
...         ...    ...      ...        ...        ...
MP          500    runtime  vendor     NMP        vendor=NewVend model=NewMod
MP          500    file     vendor     NMP        vendor=NewVend model=NewMod
```

Delete Multipathing Claim Rules

Use the `esxcli` commands to remove a multipathing PSA claim rule from the set of claim rules on the system.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. Delete a claim rule from the set of claim rules.

   ```
   esxcli storage core claimrule remove
   ```

   Note: By default, the PSA claim rule 101 masks Dell array pseudo devices. Do not delete this rule, unless you want to unmask these devices.

   The command takes the following options:

Option	Description
-c|--claimrule-class=<str>	Indicate the claim rule class (MP, Filter, VAAI).
-P|--plugin=<str>	Indicate the plug-in.
-r|--rule=<long>	Indicate the rule ID.

   This step removes the claim rule from the File class.

2. Remove the claim rule from the system.

   ```
   esxcli storage core claimrule load
   ```

   This step removes the claim rule from the Runtime class.

Mask Paths

You can prevent the host from accessing storage devices or LUNs or from using individual paths to a LUN. Use the `esxcli` commands to mask the paths. When you mask paths, you create claim rules that assign the MASK_PATH plug-in to the specified paths.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. Check what the next available rule ID is.

   ```
   esxcli storage core claimrule list
   ```

   The claim rules that you use to mask paths have rule IDs in the range from 101 through 200. If this command shows that rules 101 and 102 exist, you can specify 103 for the rule to add.
2. Assign the MASK_PATH plug-in to a path by creating a new claim rule for the plug-in.

   ```
   esxcli storage core claimrule add -P MASK_PATH
   ```
3. Load the MASK_PATH claim rule into your system.

   ```
   esxcli storage core claimrule load
   ```
4. Verify that the MASK_PATH claim rule was added correctly.

   ```
   esxcli storage core claimrule list
   ```
5. If a claim rule for the masked path exists, remove the rule.

   ```
   esxcli storage core claiming unclaim
   ```
6. Run the path claiming rules.

   ```
   esxcli storage core claimrule run
   ```

After you assign the MASK_PATH plug-in to a path, the path state becomes irrelevant and is no longer maintained by the host. As a result, commands that display the masked path's information might show the path state as dead.

Masking a LUN

In this example, you mask the LUN 20 on targets T1 and T2 accessed through storage adapters vmhba2 and vmhba3.

1. `#esxcli storage core claimrule list`
2. ```
   #esxcli storage core claimrule add -P MASK_PATH -r 109 -t location -A vmhba2 -C 0 -T 1 -L 20
   #esxcli storage core claimrule add -P MASK_PATH -r 110 -t location -A vmhba3 -C 0 -T 1 -L 20
   #esxcli storage core claimrule add -P MASK_PATH -r 111 -t location -A vmhba2 -C 0 -T 2 -L 20
   #esxcli storage core claimrule add -P MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L 20
   ```
3. `#esxcli storage core claimrule load`
4. `#esxcli storage core claimrule list`
5. ```
   #esxcli storage core claiming unclaim -t location -A vmhba2
   #esxcli storage core claiming unclaim -t location -A vmhba3
   ```
6. `#esxcli storage core claimrule run`

Unmask Paths

When you need the host to access the masked storage device, unmask the paths to the device.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Note: When you run an unclaim operation using a device property, for example, device ID or vendor, the paths claimed by the MASK_PATH plug-in are not unclaimed. The MASK_PATH plug-in does not track any device property of the paths that it claims.

1. Delete the MASK_PATH claim rule.
   ```
   esxcli storage core claimrule remove -r rule#
   ```
2. Verify that the claim rule was deleted correctly.
   ```
   esxcli storage core claimrule list
   ```
3. Reload the path claiming rules from the configuration file into the VMkernel.
   ```
   esxcli storage core claimrule load
   ```
4. Run the `esxcli storage core claiming unclaim` command for each path to the masked storage device.
   For example:
   ```
   esxcli storage core claiming unclaim -t location -A vmhba0 -C 0 -T 0 -L 149
   ```
5. Run the path claiming rules.
   ```
   esxcli storage core claimrule run
   ```

Your host can now access the previously masked storage device.

Define NMP SATP Rules

The NMP SATP claim rules define which SATP manages a storage device. Usually, you can use the default SATPs provided for storage devices. If default settings are not sufficient, use the `esxcli` commands to change the SATP for a specific device.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

You might need to create an SATP rule when you install a third-party SATP for a specific storage array.

1. To add a claim rule for a specific SATP, run the `esxcli storage nmp satp rule add` command. The command takes the following options.

Option	Description
-b|--boot	This rule is a system default rule added at boot time. Do not modify `esx.conf` or add to a host profile.
-c|--claim-option=*string*	Set the claim option string when adding a SATP claim rule.
-e|--description=*string*	Set the claim rule description when adding a SATP claim rule.
-d|--device=*string*	Set the device when adding SATP claim rules. Device rules are mutually exclusive with vendor/model and driver rules.
-D|--driver=*string*	Set the driver string when adding a SATP claim rule. Driver rules are mutually exclusive with vendor/model rules.
-f|--force	Force claim rules to ignore validity checks and install the rule anyway.
-h|--help	Show the help message.
-M|--model=*string*	Set the model string when adding SATP a claim rule. Vendor/ Model rules are mutually exclusive with driver rules.
-o|--option=*string*	Set the option string when adding a SATP claim rule.
-P|--psp=*string*	Set the default PSP for the SATP claim rule.
-O|--psp-option=*string*	Set the PSP options for the SATP claim rule.

Option	Description
-s|--satp=*string*	The SATP for which a new rule is added.
-R|--transport=*string*	Set the claim transport type string when adding a SATP claim rule.
-t|--type=*string*	Set the claim type when adding a SATP claim rule.
-V|--vendor=*string*	Set the vendor string when adding SATP claim rules. Vendor/Model rules are mutually exclusive with driver rules.

Note: When searching the SATP rules to locate a SATP for a given device, the NMP searches the driver rules first. If there is no match, the vendor/model rules are searched, and finally the transport rules. If there is still no match, NMP selects a default SATP for the device.

2. Reboot your host.

Defining an NMP SATP Rule

The following sample command assigns the VMW_SATP_INV plug-in to manage storage arrays with vendor string NewVend and model string NewMod.

```
# esxcli storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

When you run the `esxcli storage nmp satp list -s VMW_SATP_INV` command, you can see the new rule on the list of VMW_SATP_INV rules.

Scheduling Queues for Virtual Machine I/Os

By default, vSphere provides a mechanism that creates scheduling queues for every virtual machine file. Each file, for example `.vmdk`, gets its own bandwidth controls.

This mechanism ensures that I/O for a particular virtual machine file goes into its own separate queue and avoids interfering with I/Os from other files.

This capability is enabled by default. You can use the vSphere Client or the `esxcli` commands to disable or reenable the capability.

Edit Per File I/O Scheduling in the vSphere Client

The advanced `VMkernel.Boot.isPerFileSchedModelActive` parameter controls the per file I/O scheduling mechanism on VMFS and NFS 3 datastores. On the ESXi host, the mechanism is enabled by default. You can disable the mechanism using the **Advanced System Settings** dialog box.

If you turn off the per file I/O scheduling model, your host reverts to a legacy scheduling mechanism. The legacy scheduling maintains only one I/O queue for each virtual machine and storage device pair. All I/Os between the virtual machine and its virtual disks are moved into this queue. As a result, I/Os from different virtual disks might interfere with each other in sharing the bandwidth and affect each other's performance.

Note: Do not disable per file scheduling if you have the HPP plug-in and the latency sensitive threshold parameter configured for high-speed local devices. Disabling per file scheduling might cause unpredictable behavior.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4.
5. Edit the value of the **VMkernel.Boot.isPerFileSchedModelActive** parameter.

Option	Description
False	Disable the per file scheduling mechanism.
True (default)	Reenable the per file scheduling mechanism.

6. Reboot the host for the changes to take effect.

Use esxcli Commands to Enable or Disable Per File I/O Scheduling

You can use the `esxcli` commands to change the I/O scheduling capability for VMFS, NFS 3, and NFS 4.1 datastores on your ESXi host. The capability is enabled by default.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

To enable or disable per file I/O scheduling, run the following commands:

Option	Description
`esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE`	Disable per file I/O scheduling for VMFS and NFS 3.
`esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE`	Enable per file I/O scheduling for VMFS and NFS 3.
`esxcli system module parameters list -m nfs41client`	List the current status of NFS 4.1 file based scheduler
`esxcli system module parameters set -m nfs41client -p fileBasedScheduler=0`	Disable file based scheduler for NFS 4.1.
`esxcli system module parameters set -m nfs41client -p fileBasedScheduler=1`	Enable file based scheduler for NFS 4.1.

Raw Device Mapping

Raw device mapping (RDM) provides a mechanism for a virtual machine to have direct access to a LUN on the physical storage subsystem.

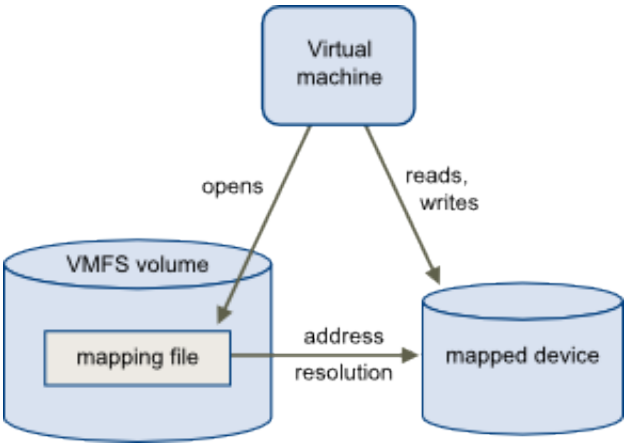
The following topics contain information about RDMs and provide instructions on how to create and manage RDMs.

About Raw Device Mapping

An RDM is a mapping file in a separate VMFS volume that acts as a proxy for a raw physical storage device. With the RDM, a virtual machine can access and use the storage device directly. The RDM contains metadata for managing and redirecting disk access to the physical device.

The file gives you some of the advantages of direct access to a physical device, but keeps some advantages of a virtual disk in VMFS. As a result, it merges the VMFS manageability with the raw device access.

Figure 79: Raw Device Mapping



Typically, you use VMFS datastores for most virtual disk storage. On certain occasions, you might use raw LUNs or logical disks located in a SAN.

For example, you might use raw LUNs with RDMs in the following situations:

- When SAN snapshot or other layered applications run in the virtual machine. The RDM enables backup offloading systems by using features inherent to the SAN.
- In any MSCS clustering scenario that spans physical hosts, such as virtual-to-virtual clusters and physical-to-virtual clusters. In this case, cluster data and quorum disks are configured as RDMs rather than as virtual disks on a shared VMFS.

Think of an RDM as a symbolic link from a VMFS volume to a raw LUN. The mapping makes LUNs appear as files in a VMFS volume. The RDM, not the raw LUN, is referenced in the virtual machine configuration. The RDM contains a reference to the raw LUN.

Two compatibility modes are available for RDMs:

- In the virtual compatibility mode, the RDM acts like a virtual disk file. The RDM can use snapshots.
- In the physical compatibility mode, the RDM offers direct access to the SCSI device for those applications that require lower-level control.

Benefits of Raw Device Mapping

An RDM provides a number of benefits, but it should not be used in every situation. In general, virtual disk files are preferable to RDMs for manageability. However, when you need raw devices, you must use the RDM.

RDM offers several benefits.

User-Friendly Persistent Names	Provides a user-friendly name for a mapped device. When you use an RDM, you do not need to refer to the device by its device name. You refer to it by the name of the mapping file, for example: `/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk`
Dynamic Name Resolution	Stores unique identification information for each mapped device. VMFS associates each RDM with its current SCSI device, regardless of changes in the physical configuration of the server because of adapter hardware changes, path changes, device relocation, and so on.
Distributed File Locking	Makes it possible to use VMFS distributed locking for raw SCSI devices. Distributed locking on an RDM makes it safe to use a shared raw LUN without losing data when two virtual machines on different servers try to access the same LUN.

File Permissions

Makes file permissions possible. The permissions of the mapping file are enforced at file-open time to protect the mapped volume.

File System Operations

Makes it possible to use file system utilities to work with a mapped volume, using the mapping file as a proxy. Most operations that are valid for an ordinary file can be applied to the mapping file and are redirected to operate on the mapped device.

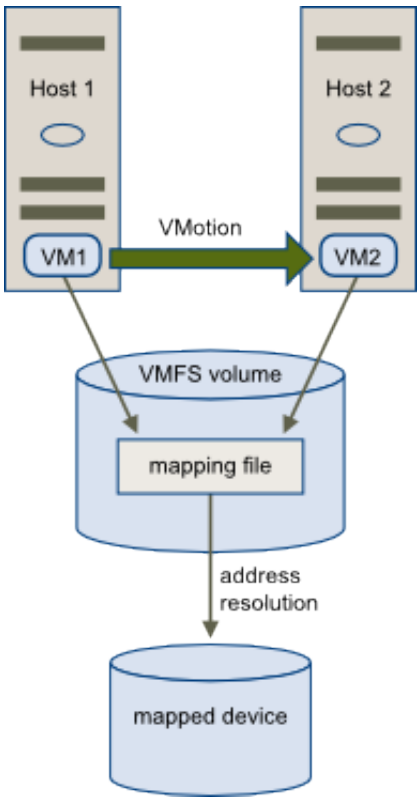
Snapshots

Makes it possible to use virtual machine snapshots on a mapped volume. Snapshots are not available when the RDM is used in physical compatibility mode.

vMotion

Lets you migrate a virtual machine with vMotion. The mapping file acts as a proxy to allow vCenter Server to migrate the virtual machine by using the same mechanism that exists for migrating virtual disk files.

Figure 80: vMotion of a Virtual Machine Using Raw Device Mapping



SAN Management Agents

Makes it possible to run some SAN management agents inside a virtual machine. Similarly, any software that needs to access a device by using hardware-specific SCSI commands can be run in a virtual machine. This kind of software is called SCSI target-based software. When you use SAN management agents, select a physical compatibility mode for the RDM.

N-Port ID Virtualization (NPIV)

Makes it possible to use the NPIV technology that allows a single Fibre Channel HBA port to register with the Fibre Channel fabric using several worldwide port names (WWPNs). This ability makes the HBA port appear as multiple virtual ports, each having its own ID and virtual port name. Virtual machines can then claim each of these virtual ports and use them for all RDM traffic.

Note: You can use NPIV only for virtual machines with RDM disks.

VMware works with vendors of storage management software to ensure that their software functions correctly in environments that include ESXi. Some applications of this kind are:

- SAN management software
- Storage resource management (SRM) software
- Snapshot software
- Replication software

Such software uses a physical compatibility mode for RDMs so that the software can access SCSI devices directly.

Various management products are best run centrally (not on the ESXi machine), while others run well on the virtual machines. VMware does not certify these applications or provide a compatibility matrix. To find out whether a SAN management application is supported in an ESXi environment, contact the SAN management software provider.

RDM Considerations and Limitations

Certain considerations and limitations exist when you use RDMs.

- The RDM is not available for direct-attached block devices or certain RAID devices. The RDM uses a SCSI serial number to identify the mapped device. Because block devices and some direct-attach RAID devices do not export serial numbers, they cannot be used with RDMs.
- If you are using the RDM in physical compatibility mode, you cannot use a snapshot with the disk. Physical compatibility mode allows the virtual machine to manage its own, storage-based, snapshot or mirroring operations. Virtual machine snapshots are available for RDMs with virtual compatibility mode.
- You cannot map to a disk partition. RDMs require the mapped device to be a whole LUN.
- If you use vMotion to migrate virtual machines with RDMs, make sure to maintain consistent LUN IDs for RDMs across all participating ESXi hosts.

Raw Device Mapping Characteristics

An RDM is a special mapping file in a VMFS volume that manages metadata for its mapped device. The mapping file is presented to the management software as an ordinary disk file, available for the usual file-system operations. To the virtual machine, the storage virtualization layer presents the mapped device as a virtual SCSI device.

Key contents of the metadata in the mapping file include the location of the mapped device (name resolution), the locking state of the mapped device, permissions, and so on.

RDM Virtual and Physical Compatibility Modes

You can use RDMs in virtual compatibility or physical compatibility modes. Virtual mode specifies full virtualization of the mapped device. Physical mode specifies minimal SCSI virtualization of the mapped device, allowing the greatest flexibility for SAN management software.

In virtual mode, the VMkernel sends only READ and WRITE to the mapped device. The mapped device appears to the guest operating system exactly the same as a virtual disk file in a VMFS volume. The real hardware characteristics are hidden. If you are using a raw disk in virtual mode, you can realize the benefits of VMFS such as advanced file locking for data protection and snapshots for streamlining development processes. Virtual mode is also more portable across storage hardware than physical mode, presenting the same behavior as a virtual disk file.

In physical mode, the VMkernel passes all SCSI commands to the device, with one exception: the REPORT LUNs command is virtualized so that the VMkernel can isolate the LUN to the owning virtual machine. Otherwise, all physical characteristics of the underlying hardware are exposed. Physical mode is useful to run SAN management agents or

other SCSI target-based software in the virtual machine. Physical mode also allows virtual-to-physical clustering for cost-effective high availability.

VMFS5 and VMFS6 support greater than 2 TB disk size for RDMs in virtual and physical modes.

Dynamic Name Resolution

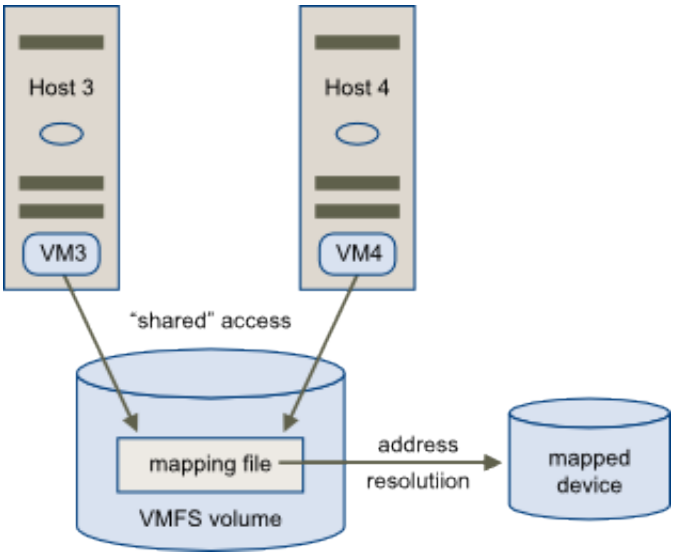
The RDM file supports dynamic name resolution when a path to a raw device changes.

VMFS uniquely identifies all mapped storage devices, and the identification is stored in its internal data structures. Any change in the path to a raw device, such as a Fibre Channel switch failure or the addition of a new HBA, can change the device name. Dynamic name resolution resolves these changes and automatically associates the original device with its new name.

Raw Device Mapping with Virtual Machine Clusters

Use an RDM with virtual machine clusters that require access to the same raw LUN for failover scenarios. The setup is similar to that of a virtual machine cluster that accesses the same virtual disk file, but an RDM replaces the virtual disk file.

Figure 81: Access from Clustered Virtual Machines



Comparing Available SCSI Device Access Modes

The ways of accessing a SCSI-based storage device include a virtual disk file on a VMFS datastore, virtual mode RDM, and physical mode RDM.

The following table provides a comparison of features available with the different modes.

Table 223: Features Available with Virtual Disks and Raw Device Mappings

ESXi Features	Virtual Disk File	Virtual Mode RDM	Physical Mode RDM
SCSI Commands Passed Through	No	No	Yes `REPORT LUNs` is not passed through
vCenter Server Support	Yes	Yes	Yes

ESXi Features	Virtual Disk File	Virtual Mode RDM	Physical Mode RDM
Snapshots	Yes	Yes	No
Distributed Locking	Yes	Yes	Yes
Clustering	Cluster-in-a-box only	Cluster-in-a-box cluster-across-boxes	Physical-to-virtual clustering cluster-across-boxes
SCSI Target-Based Software	No	No	Yes

Use virtual disk files for the cluster-in-a-box type of clustering. If you plan to reconfigure your cluster-in-a-box clusters as cluster-across-boxes clusters, use virtual mode RDMs for the cluster-in-a-box clusters.

Create Virtual Machines with RDMs

When you give your virtual machine direct access to a raw SAN LUN, you create an RDM disk that resides on a VMFS datastore and points to the LUN. You can create the RDM as an initial disk for a new virtual machine or add it to an existing virtual machine. When creating the RDM, you specify the LUN to be mapped and the datastore on which to put the RDM.

Although the RDM disk file has the same `.vmdk` extension as a regular virtual disk file, the RDM contains only mapping information. The actual virtual disk data is stored directly on the LUN.

This procedure assumes that you are creating a new virtual machine. For information, see the *vSphere Virtual Machine Administration* documentation.

1. Create a virtual machine.
   a) Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.
   b) Select **Create a new virtual machine** and click **Next**.
   c) Follow the steps required to create a virtual machine.
2. On the Customize Hardware page, click the **Virtual Hardware** tab.
3. Optional: To delete the default virtual hard disk that the system created for your virtual machine, move your cursor over the disk and click the **Remove** icon.
4. Add an RDM disk.
   a) Click **Add New Devices** and select **RDM Disk** from the list.
   b) From the list of LUNs, select a target raw LUN and click **OK**.

      The system creates an RDM disk that maps your virtual machine to the target LUN. The RDM disk is shown on the list of virtual devices as a new hard disk.

5. Configure the RDM disk.
   a) Click the **New Hard Disk** triangle to expand the properties for the RDM disk.
   b) Select a location for the RDM.

      You can place the RDM on the same datastore where your virtual machine configuration files reside, or select a different datastore.

      Note: To use vMotion for virtual machines with enabled NPIV, make sure that the RDM files and the virtual machine files are located on the same datastore. You cannot perform Storage vMotion when NPIV is enabled.
   c) Select a compatibility mode.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, made into a template, or migrated if the migration involves copying the disk.
Virtual	Allows the RDM to behave as if it were a virtual disk, so you can use such features as taking snapshots, cloning, and so on. When you clone the disk or make a template out of it, the contents of the LUN are copied into a `.vmdk` virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN into a virtual disk.

   d) If you selected virtual compatibility mode, select a disk mode.

      Disk modes are not available for RDM disks using physical compatibility mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

6. Complete your virtual machine configuration.

Manage Paths for a Mapped LUN

When you use virtual machines with RDMs, you can manage paths for mapped raw LUNs.

1. Right-click the virtual machine and select **Edit Settings**.
2. Click the **Virtual Hardware** tab and click **Hard Disk** to expand the disk options menu.
3. Click the device ID that appears next to **Physical LUN** to open the **Edit Multipathing Policies** dialog box.
4. Use the **Edit Multipathing Policies** dialog box to enable or disable paths, set multipathing policy, and specify the preferred path.

   For information on managing paths, see Understanding Multipathing and Failover.

Virtual Machines with RDMs Must Ignore SCSI INQUIRY Cache

Certain virtual machines with RDMs must obtain the SCSI INQUIRY information from the LUN instead of using SCSI INQUIRY data cached by ESXi.

Certain guest operating systems or applications that run in the virtual machines with the RDMs display unpredictable behavior.

This behavior might be caused by cached SCSI INQUIRY data that interferes with specific guest operating systems and applications.

When the ESXi host first connects to a target storage device, it issues the SCSI INQUIRY command to obtain basic identification data from the device. By default, ESXi caches the received SCSI INQUIRY data (Standard, page 80, and page 83), and the data remains unchanged afterwards. Responses for subsequent SCSI INQUIRY commands are returned from the cache.

However, specific guest operating systems running in virtual machines with RDMs must query the LUN instead of using SCSI INQUIRY data cached by ESXi. In these cases, you can configure the VM to ignore the SCSI INQUIRY cache.

Use one of the following methods.

Option	Description
Modify the .vmx file of the virtual machine with the RDM	Use this method for the VMs with hardware version 8 or later. 1. Add the following parameter to the file: `scsi`*`x`*`:`*`y`*`.ignoreDeviceInquiryCache = "true"` where *x* is the SCSI controller number and *y* is the SCSI target number of the RDM. 2. Reboot the VM.
Use the `esxcli` command	Because you configure the setting at a host level, no VM hardware version limitations apply. `esxcli storage core device inquirycache set --device` *`device id`* `--ignore true` No VM reboot is required.

No matter which method you use to set the SCSI INQUIRY cache parameter to true, the VM starts contacting the LUN directly for the SCSI INQUIRY data.

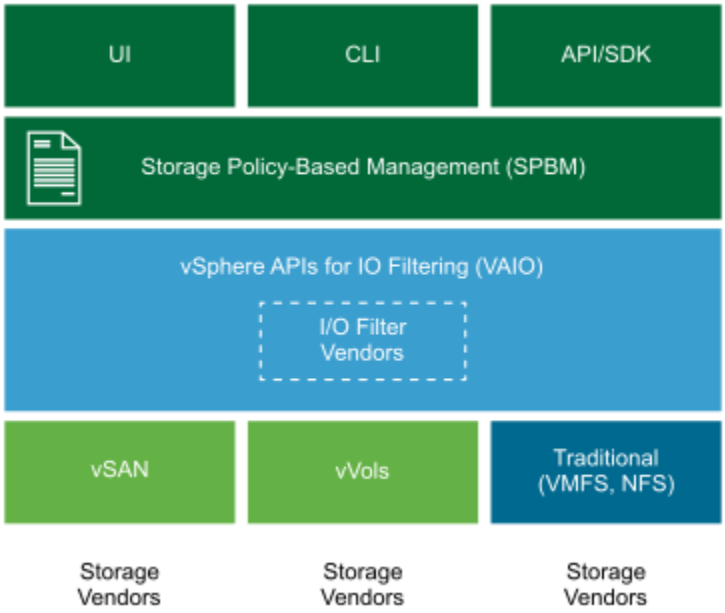
ignoreDeviceInquiryCache parameter in vmx	ignore inquirycache parameter in esxcli	Inquiry request serviced from
True	True	LUN
False (default if the parameter is not present)	True	LUN
True	False	LUN
False (default if the parameter is not present)	False	Cache

Storage Policy Based Management

Within a software-defined data center, Storage Policy Based Management (SPBM) plays a major role by helping to align storage with application demands of your virtual machines. It provides a storage policy framework that serves as a single unified control panel across a broad range of data services and storage solutions.

As an abstraction layer, SPBM abstracts storage services delivered by Virtual Volumes, vSAN, I/O filters, or other storage entities.

Rather than integrating with each individual type of storage and data services, SPBM provides a universal framework for different types of storage entities.



SPBM offers the following mechanisms:

- Advertisement of storage capabilities and data services that storage arrays and other entities, such as I/O filters, offer.
- Bidirectional communications between ESXi and vCenter Server on one side, and storage arrays and entities on the other.
- Virtual machine provisioning based on VM storage policies.

Virtual Machine Storage Policies

Virtual machine storage policies are essential to virtual machine provisioning through SPBM. The policies control which type of storage is provided for the virtual machine and how the virtual machine is placed within storage. They also determine data services that the virtual machine can use.

vSphere offers default storage policies. In addition, you can define policies and assign them to the virtual machines.

You use the VM Storage Policies interface to create a storage policy. When you define the policy, you specify various storage requirements for applications that run on the virtual machines. You can also use storage policies to request specific data services, such as caching or replication, for virtual disks.

You apply the storage policy when you create, clone, or migrate the virtual machine. After you apply the storage policy, the SPBM mechanism assists you with placing the virtual machine in a matching datastore. In certain storage environments, SPBM determines how the virtual machine storage objects are provisioned and allocated within the storage resource to guarantee the required level of service. The SPBM also enables requested data services for the virtual machine and helps you to monitor policy compliance.

Workflow for Virtual Machine Storage Policies

The entire process of creating and managing storage policies typically includes several steps.

Whether you must perform a specific step might depend on the type of storage or data services that your environment offers.

Step	Description
Populate the VM Storage Policies interface with appropriate data.	The VM Storage Policies interface is populated with information about datastores and data services that are available in your storage environment. This information is obtained from storage providers and datastore tags. • For entities represented by storage providers, verify that an appropriate provider is registered. Entities that use the storage provider include vSAN, Virtual Volumes, and I/O filters. Depending on the type of storage entity, some providers are self-registered. Other providers must be manually registered. See Use Storage Providers to Populate the VM Storage Policies Interface and Register Storage Providers for Virtual Volumes. • Tag datastores that are not represented by storage providers. You can also use tags to indicate a property that is not communicated through the storage provider, such as geographical location or administrative group. See Assign Tags to Datastores.
Create predefined storage policy components.	A storage policy component describes a single data service, such as replication, that must be provided for the virtual machine. You can define the component in advance and associate it with multiple VM storage policies. The components are reusable and interchangeable. See Create Storage Policy Components.
Create VM storage policies.	When you define storage policies for virtual machines, you specify storage requirements for applications that run on the virtual machines. See Creating and Managing VM Storage Policies.
Apply the VM storage policy to the virtual machine.	You can apply the storage policy when deploying the virtual machine or configuring its virtual disks. See Assign Storage Policies to Virtual Machines.
Check compliance for the VM storage policy.	Verify that the virtual machine uses the datastore that is compliant with the assigned storage policy. See Check Compliance for a VM Storage Policy.

To create and manage your storage policies, you use the VM Storage Policy interface of the vSphere Client.

Populating the VM Storage Policies Interface

Before you start creating VM storage policies, you must populate the VM Storage Policy interface with information about storage entities and data services that are available in your storage environment.

This information is obtained from storage providers, also called VASA providers. Another source is datastore tags.

Storage Capabilities and Services

Certain datastores, for example, Virtual Volumes and vSAN, are represented by the storage providers. Through the storage providers, the datastores can advertise their capabilities in the VM Storage Policy interface. These datastore capabilities, data

	services, and other characteristics with ranges of values populate the VM Storage Policy interface. You use these characteristics when you define datastore-based placement and service rules for your storage policy.
Data Services	I/O filters on your hosts are also represented by the storage providers. The storage provider delivers information about the data services of the filters to the VM Storage Policy interface. You use this information when defining the rules for host-based data services, also called common rules. Unlike the datastore-specific rules, these rules do not define storage placement and storage requirements for the virtual machine. Instead, they activate the requested I/O filter data services for the virtual machine.
Tags	Generally, VMFS and NFS datastores are not represented by a storage provider. They do not display their capabilities and data services in the VM Storage Polices interface. You can use tags to encode information about these datastores. For example, you can tag your VMFS datastores as VMFS-Gold and VMFS-Silver to represent different levels of service. For Virtual Volumes and vSAN datastores, you can use tags to encode information that is not advertised by the storage provider, such as geographical location (Palo Alto), or administrative group (Accounting). Similar to the storage capabilities and characteristics, all tags associated with the datastores appear in the VM Storage Policies interface. You can use the tags when you define the tag-based placement rules.

Use Storage Providers to Populate the VM Storage Policies Interface

For entities represented by storage (VASA) providers, verify that an appropriate provider is registered. After the storage providers are registered, the VM Storage Policies interface becomes populated with information about datastores and data services that the providers represent.

Register the storage providers that require manual registration. For more information, see the appropriate documentation:

- *Administering VMware vSAN*
- Working with VMware vSphere Virtual Volumes
- Filtering Virtual Machine I/O

Entities that use the storage provider include vSAN, Virtual Volumes, and I/O filters. Depending on the type of the entity, some providers are self-registered. Other providers, for example, the Virtual Volumes storage provider, must be manually registered. After the storage providers are registered, they deliver the following data to the VM Storage Policies interface:

- Storage capabilities and characteristics for such datastores as Virtual Volumes and vSAN.
- Data services the I/O filters provide.

1. Browse to the vCenter Server instance.
2. Click the **Configure** tab, and click **Storage Providers**.
3. In the Storage Providers list, view the storage providers registered with vCenter Server.

   The list shows general information including the name of the storage provider, its URL and status, storage entities that the provider represents, and so on.

4. To display more details, select a specific storage provider or its component from the list.

Assign Tags to Datastores

Use tags to encode information about a datastore. The tags are helpful when your datastore is not represented by a storage provider and does not advertise its services in the VM Storage Polices interface. You can also use the tags to indicate a property that is not communicated through a storage provider, such as a geographical location or administrative group.

Required privileges:

- **vSphere Tagging** > **Create vSphere Tag** on the root vCenter Server instance
- **vSphere Tagging** > **Create vSphere Tag Category** on the root vCenter Server instance
- **vSphere Tagging** > **Assign or Unassign vSphere Tag** on the root vCenter Server instance

You can apply a new tag that contains general storage information to a datastore. For more details about the tags, their categories, and how to manage the tags, see the *vCenter Server and Host Management* documentation.

1. In the vSphere Client, create a category for storage tags.
   a) From the Home menu, click **Tags & Custom Attributes**.
   b) Click the **Tags** tab and click **Categories**.
   c) Click the **Add Category** icon.
   d) Specify the category properties. See the following example.

Category Property	Example
Category Name	Storage Location
Description	Category for tags related to location of storage
Tags Per Object	**Many tags**
Associable Object Types	**Datastore** and **Datastore Cluster**

   e) Click **OK**.
2. Create a storage tag.
   a) On the **Tags** tab, click **Tags**.
   b) Click the **Add Tag** icon.
   c) Specify the properties for the tag. See the following example.

Tag Property	Example
Name	Texas
Description	Datastore located in Texas
Category	Storage Location

   d) Click **OK**.
3. Apply the tag to the datastore.
   a) Navigate to the datastore.
   b) Right-click the datastore, and select **Tags & Custom Attributes** > **Assign Tag**.
   c) From the list of tags, select an appropriate tag, for example, Texas in the Storage Location category, and click **Assign**.

The new tag is assigned to the datastore and appears on the datastore **Summary** tab in the **Tags** pane.

When creating a VM storage policy, you can reference the tag to include the tagged datastore in the list of compatible storage resources. See Create a VM Storage Policy for Tag-Based Placement.

Or you can exclude the tagged datastore from the VM storage policy. For example, your VM storage policy can include Virtual Volumes datastores located in Texas and California, but exclude datastores located in Nevada.

To learn more about how to use tags in VM storage policies, watch the following video.

About Rules and Rule Sets

After the VM Storage Policies interface is populated with the appropriate data, you can start creating your storage policies. Creating a policy involves defining specific storage placement rules and rules to configure data services.

Rules	The rule is a basic element of the VM storage policy. Each individual rule is a statement that describes a single requirement for virtual machine storage and data services.
Rule Sets	Within a storage policy, individual rules are organized into collections of rules, or rule sets. Typically, the rule sets can be in one of the following categories: rules for host-based services and datastore-specific rules.
Datastore-Specific Rule Sets	Each rule set must include placement rules that describe requirements for virtual machine storage resources. All placement rules within a single rule set represent a single storage entity. These rules can be based on storage capabilities or tags. In addition, the datastore-specific rule set can include optional rules or storage policy components that describe data services to provide for the virtual machine. Generally, these rules request such services as caching, replication, other services provided by storage systems. To define the storage policy, one datastore-specific set is required. Additional rule sets are optional. A single policy can use multiple sets of rules to define alternative storage placement parameters, often from several storage providers.
Placement Rules: Capability-Based	Placement rules specify a particular storage requirement for the VM and enable SPBM to distinguish compatible datastores among all datastores in the inventory. These rules also describe how the virtual machine storage objects are allocated within the datastore to receive the required level of service. For example, the rules can list Virtual Volumes as a destination and define the maximum recovery point objective (RPO) for the Virtual Volumes objects. When you provision the virtual machine, these rules guide the decision that SPBM makes about the virtual machine placement. SPBM finds the Virtual Volumes datastores that can match the rules and satisfy the storage requirements of the virtual machine. See Create a VM Storage Policy for Virtual Volumes.
Placement Rules: Tag-Based	Tag-based rules reference datastore tags. These rules can define the VM placement, for example, request as a target all datastores with the VMFS-Gold tag. You can also use the tag-based rules to fine-tune your VM placement request further. For example, exclude datastores with the Palo Alto tag from the list of your Virtual Volumes datastores. See Create a VM Storage Policy for Tag-Based Placement.

Rules for Host-Based Services	This rule set activates data services provided by the host. The set for host-based services can include rules or storage policy components that describe particular data services, such as encryption or replication. Unlike datastore-specific rules, this set does not include placement rules. Rules for host-based services are generic for all types of storage and do not depend on the datastore. See Create a VM Storage Policy for Host-Based Data Services.

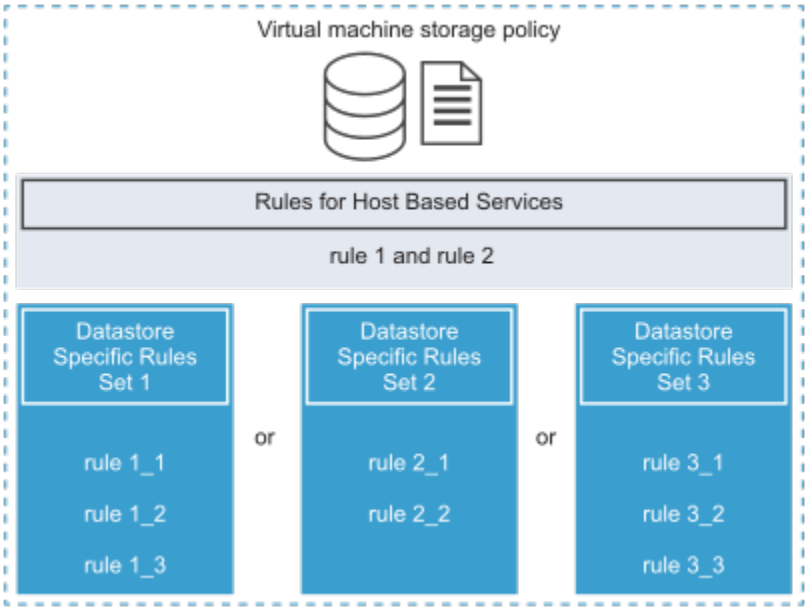
Table 224: Structure of a VM Storage Policy

Rules for Host-Based Services	Datastore-Specific Rule Sets
Rules or predefined storage policy components to activate data services installed on ESXi hosts. For example, replication by I/O filters.	Capability-based or tag-based placement rules that describe requirements for virtual machine storage resources. For example, Virtual Volumes placement.
	Rules or predefined storage policy components that activate data services provided by storage. For example, caching by Virtual Volumes.

Relationships Between Rules and Rule Sets

The boolean operator `OR` defines the relationship between the datastore-specific rule sets within the policy. The `AND` operator defines the relationship between all rules within a single rule set. The policy can contain only a rule set for host-based services, or only a datastore-specific rule set, or both.

If the rule set for host-based services is not present, meeting all the rules of a single datastore-specific rule set is sufficient to satisfy the entire policy. If the rule set for host-based services is present, the policy matches the datastore that satisfies the host services rules and all rules in one of the datastore-specific sets.



Creating and Managing VM Storage Policies

To create and manage storage policies for your virtual machines, you use the VM Storage Policies interface.

Create a VM Storage Policy for Host-Based Data Services

To define the VM storage policy in the vSphere Client, use the **Create VM Storage Policy** wizard. In this task, you create rules for data services offered by ESXi hosts. The VM storage policy that includes these rules activates specified data services for the virtual machine.

- For information about encrypting your virtual machines, see the *vSphere Security* documentation.
- For information about I/O filters, see Filtering Virtual Machine I/O.
- For information about storage policy components, see About Storage Policy Components.
- Required privileges: **VM storage policies** > **Update** and **VM storage policies** > **View**.

Available data services include encryption, I/O control, caching, and so on. Certain data services, such as encryption, are provided by VMware. Others can be offered by third-party I/O filters that you install on your host.

The data services are usually generic for all types of storage and do not depend on a datastore. Adding datastore-specific rules to the storage policy is optional.

If you add datastore-specific rules, and both the I/O filters on the host and storage offer the same type of service, for example, encryption, your policy can request this service from both providers. As a result, the virtual machine data is encrypted twice, by the I/O filter and your storage. However, replication provided by Virtual Volumes and replication provided by the I/O filter cannot coexist in the same storage policy.

1. Open the **Create VM Storage Policy** wizard.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**
   c) Click **Create**.
2. Enter the policy name and description, and click **Next**.

Option	Action
vCenter Server	Select the vCenter Server instance.
Name	Enter the name of the storage policy.
Description	Enter the description of the storage policy.

3. On the **Policy structure** page under **Host based services**, enable host based rules.
4. On the **Host based services** page, define rules to enable and configure data services provided by your host.
   a) Click the tab for the data service category, for example, **Replication**.
   b) Define custom rules for the data service category or use predefined components.

Option	Description
Disabled	Host-based services are disabled by default.
Use storage policy component	Select a storage policy component from the drop-down menu. This option is available only if you have predefined components in your database.
Custom	Define custom rules for the data service category by specifying an appropriate provider and values for the rules.

Note: You can enable several data services. If you use encryption with other data services, set the **Allow I/O filters before encryption** parameter to **True**, so that other services, such as replication, can analyze clear text data before it is encrypted.

5. On the **Storage compatibility** page, review the list of datastores that match this policy.

   To be compatible with the policy for host-based services, datastores must be connected to the host that provides these services. If you add datastore-specific rule sets to the policy, the compatible datastores must also satisfy storage requirements of the policy.

6. On the **Review and finish** page, review the storage policy settings and click **Finish**.

   To change any settings, click **Back** to go to the relevant page.

The new VM storage policy for host-based data services appears on the list.

Create a VM Storage Policy for Virtual Volumes

To define the VM storage policy in the vSphere Client, use the **Create VM Storage Policy** wizard. In this task, you create a custom storage policy compatible with Virtual Volumes. When you define the VM storage policy for Virtual Volumes, you create rules to configure storage and data services provided by the Virtual Volumes datastore. The rules are applied when the VM is placed on the Virtual Volumes datastore. The custom storage policy can replace the default No Requirements storage policy for Virtual Volumes that VMware provides.

- Verify that the Virtual Volumes storage provider is available and active. See Register Storage Providers for Virtual Volumes.
- Make sure that the VM Storage Policies interface is populated with information about storage entities and data services that are available in your storage environment. See Populating the VM Storage Policies Interface.
- Define appropriate storage policy components. See Create Storage Policy Components.
- Required privileges: **VM storage policies** > **Update** and **VM storage policies** > **View**.

The procedure assumes that you are creating the VM storage policy for Virtual Volumes. For information about the vSAN storage policy, see the *Administering VMware vSAN* documentation.

1. Open the **Create VM Storage Policy** wizard.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**.
   c) Click **Create**.
2. Enter the policy name and description, and click **Next**.

Option	Action
vCenter Server	Select the vCenter Server instance.
Name	Enter the name of the storage policy, for example Virtual Volumes Storage Policy.
Description	Enter the description of the storage policy.

3. On the **Policy structure** page under Datastore specific rules, enable rules for a target storage entity, such as Virtual Volumes storage.

   You can enable rules for several datastores. Multiple rule sets allow a single policy to define alternative storage placement parameters, often from several storage providers.

4. On the *Virtual Volumes* rules page, define storage placement rules for the target Virtual Volumes datastore.
   a) Click the **Placement** tab and click **Add Rule**.
   b) From the Add Rule drop-down menu, select available capability and specify its value.
      For example, you can specify the number of read operations per second for the Virtual Volumes objects.
      You can include as many rules as you need for the selected storage entity. Verify that the values you provide are within the range of values that the Virtual Volumes datastore advertises.
   c) To fine-tune your placement request further, click the **Tags** tab and add a tag-based rule.
      Tag-based rules can filter datastores by including or excluding specific placement criteria. For example, your VM storage policy can include Virtual Volumes datastores located in Texas and California, but exclude datastores located in Nevada.
5. Optional: Define rules to configure datastore-specific services.
   The data services, such as encryption, caching, or replication, are offered by the storage. The VM storage policy that references data services, requests these services for the VM when the VM is placed to the Virtual Volumes datastore.
   a) Click the tab for the data service category, for example, **Replication**.
   b) Define custom rules for the data service category or use predefined components.

Option	Description
Disabled	Datastore-specific services are disabled by default.
Use storage policy component	Select a storage policy component from the drop-down menu. This option is available only if you have predefined components in your database.
Custom	Define custom rules for the data service category by specifying an appropriate provider and values for the rules.

6. On the **Storage compatibility** page, review the list of datastores that match this policy.
   If the policy includes several rule sets, the datastore must satisfy at least one rule set and all rules within this set.
7. On the **Review and finish** page, review the storage policy settings and click **Finish**.
   To change any settings, click **Back** to go to the relevant page.

The new VM storage policy compatible with Virtual Volumes appears on the list.

You can now associate this policy with a virtual machine, or designate the policy as default.

Create a VM Storage Policy for Tag-Based Placement

Tag-based rules reference the tags that you assign to the datastores and can filter the datastores to be used for placement of the VMs. To define tag-based placement in the vSphere Client, use the **Create VM Storage Policy** wizard.

- Make sure that the VM Storage Policies interface is populated with information about storage entities and data services that are available in your storage environment. See Populating the VM Storage Policies Interface.

- Required privileges: **VM storage policies** > **Update** and **VM storage policies** > **View**.

Note: At a datastore cluster level, you can use a tag-based storage policy only when all datastores in the cluster have consistent tags.

1. Open the **Create VM Storage Policy** wizard.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**.
   c) Click **Create**.
2. Enter the policy name and description, and click **Next**.

Option	Action
vCenter Server	Select the vCenter Server instance.
Name	Enter the name of the storage policy.
Description	Enter the description of the storage policy.

3. On the **Policy structure** page under Datastore specific rules, enable tag-based placement rules.
4. On the **Tag based placement** page, create the tag rules.
   a) Click **Add Tag Rule** and define tag-based placement criteria. Use the following as an example.

Option	Example
Tag category	Level of Service
Usage option	Use storage tagged with
Tags	Gold

   All datastores with the Gold tag become compatible as the storage placement target.
   b) Optional: Add more tag-based rules.
5. On the **Storage compatibility** page, review the list of datastores that match this policy.
6. On the **Review and finish** page, review the storage policy settings and click **Finish**.
   To change any settings, click **Back** to go to the relevant page.

The new VM storage policy compatible with tagged datastores appears on the list.

Edit or Clone a VM Storage Policy

If storage requirements for virtual machines and virtual disks change, you can modify the existing storage policy. You can also create a copy of the existing VM storage policy by cloning it. While cloning, you can optionally select to customize the original storage policy.

Required privilege: **StorageProfile.View**

1. In the vSphere Client, navigate to the storage policy.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**.
2. Select the storage policy, and click one of the following icons:
   - **Edit**
   - **Clone**

3. Optional: Modify the policy and click **OK**.
4. If editing the storage policy that is used by a virtual machine, reapply the policy to the virtual machine.

Option	Description
Manually later	If you select this option, the compliance status for all virtual disks and virtual machine home objects associated with the storage policy changes to Out of Date. To update configuration and compliance, manually reapply the storage policy to all associated entities. See Reapply Virtual Machine Storage Policy.
Now	Update virtual machine and compliance status immediately after editing the storage policy.

About Storage Policy Components

A VM storage policy can include one or several reusable and interchangeable building blocks, called storage policy components. Each component describes a particular data service to be provided for the virtual machine. You can define the policy components in advance and associate them with multiple VM storage policies.

You cannot assign the predefined component directly to a virtual machine or virtual disk. Instead, you must add the component to the VM storage policy, and assign the policy to the virtual machine.

The component describes one type of service from one service provider. The services can vary depending on the providers that you use, but generally belong in one of the following categories.

- Compression
- Caching
- Encryption
- Replication

When you create the storage policy component, you define the rules for one specific type and grade of service.

The following example shows that virtual machines VM1 and VM2 have identical placement requirements, but must have different grades of replication services. You can create the storage policy components with different replication parameters and add these components to the related storage policies.

Table 225: Storage Policy Components

Virtual Machine	Placement Rules	Storage Policy Component
VM1 requires replication every 2 hours	Virtual Volumes Datastore	2-hour Replication
VM2 requires replication every 4 hours	Virtual Volumes Datastore	4-hour Replication

The provider of the service can be a storage system, an I/O filter, or another entity. If the component references an I/O filter, the component is added to the host-based rules of the storage policy. Components that reference entities other than the I/O filters, for example, a storage system, are added to the datastore-specific rule sets.

When you work with the components, follow these guidelines:

- Each component can include only one set of rules. All characteristics in this rule set belong to a single provider of the data services.
- If the component is referenced in the VM storage policy, you cannot delete the component. Before deleting the component, you must remove it from the storage policy or delete the storage policy.
- When you add components to the policy, you can use only one component from the same category, for example caching, per a set of rules.

Create Storage Policy Components

A storage policy component describes a single data service, such as replication, that must be provided for the virtual machine. You can define the component in advance and associate it with multiple VM storage policies. The components are reusable and interchangeable.

1. In the vSphere Client, open the **New Storage Policy Component** dialog box.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **Storage Policy Components**.
2. Click **Create Storage Policy Component**.
3. Select the vCenter Server instance.
4. Enter a name, for example, 4-hour Replication, and a description for the policy component.
   Make sure that the name does not conflict with the names of other components or storage policies.
5. Select the category of the service, for example, **Replication**.
6. Select the service provider.
7. Define rules for the selected category.
   For example, if you are configuring 4-hour replication, set the Recovery Point Objective (RPO) value to 4.

   For encryption based on I/O filters, set the **Allow I/O filters before encryption** parameter. Encryption provided by storage does not require this parameter.

Option	Description
False (default)	Does not allow the use of other I/O filters before the encryption filter.
True	Allows the use of other I/O filters before the encryption filter. Other filters, such as replication, can analyze clear text data before it is encrypted.

8. Click **OK**.

The new component appears in the list of storage policy components.

You can add the component to the VM storage policy. If the data service that the component references is provided by the I/O filters, you add the component to the host-based rules of the storage policy. Components that reference entities other than the I/O filters, for example, a storage system, are added to the datastore-specific rule sets.

Edit or Clone Storage Policy Components

You can modify the existing storage policy components. You can also create a copy of the existing component by cloning it.

1. In the vSphere Client, navigate to the storage policy component to edit or clone.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **Storage Policy Components**.
2. Select the component and click one of the following icons.

Option	Description
Edit Settings	When editing, you cannot change the category of the data service and the provider. For example, if the original component references replication provided by I/O filters, these settings must remain unchanged.

Option	Description
Clone	When cloning, you can customize any settings of the original component.

3. Modify appropriate values, and click **OK**.
4. If a VM storage policy that is assigned to a virtual machine references the policy component you edit, reapply the storage policy to the virtual machine.

Menu Item	Description
Manually later	If you select this option, the compliance status for all virtual disks and virtual machine home objects associated with the storage policy changes to Out of Date. To update configuration and compliance, manually reapply the storage policy to all associated entities. See Reapply Virtual Machine Storage Policy.
Now	Update virtual machine and compliance status immediately after editing the storage policy.

Storage Policies and Virtual Machines

After you define a VM storage policy, you can apply it to a virtual machine. You apply the storage policy when provisioning the virtual machine or configuring its virtual disks. Depending on its type and configuration, the policy might serve different purposes. The policy can select the most appropriate datastore for the virtual machine and enforce the required level of service. Or it can enable specific data services for the virtual machine and its disks.

If you do not specify the storage policy, the system uses a default storage policy that is associated with the datastore. If your storage requirements for the applications on the virtual machine change, you can modify the storage policy that was originally applied to the virtual machine.

Assign Storage Policies to Virtual Machines

You can assign a VM storage policy in an initial deployment of a virtual machine or when you perform other virtual machine operations, such as cloning or migrating.

This topic describes how to assign the VM storage policy when you create a virtual machine. For information about other deployment methods that include cloning, deployment from a template, and so on, see the *vSphere Virtual Machine Administration* documentation.

You can apply the same storage policy to the virtual machine configuration file and all its virtual disks. If storage requirements for your virtual disks and the configuration file are different, you can associate different storage policies with the VM configuration file and the selected virtual disks.

1. Start the virtual machine provisioning process and follow the appropriate steps.
2. Assign the same storage policy to all virtual machine files and disks.
   a) On the **Select storage** page, select a storage policy from the **VM Storage Policy** drop-down menu.

      Based on its configuration, the storage policy separates all datastores into compatible and incompatible. If the policy references data services offered by a specific storage entity, for example, Virtual Volumes, the compatible list includes datastores that represent only that type of storage.
   b) Select an appropriate datastore from the list of compatible datastores.

      The datastore becomes the destination storage resource for the virtual machine configuration file and all virtual disks.
   c) If you use the replication service with Virtual Volumes, specify the replication group.

      Replication groups indicate which VMs and virtual disks must be replicated together to a target site.

Option	Description
Preconfigured replication group	Replication groups that are configured in advance on the storage side. vCenter Server and ESXi discover the replication groups, but do not manage their life cycle.
Automatic replication group	Virtual Volumes creates a replication group and assigns all VM objects to this group.

3. Change the VM storage policy for the virtual disk.

   Use this option if requirements for storage placement are different for virtual disks. You can also use this option to enable I/O filter services, such as caching and replication, for your virtual disks.
   a) On the **Customize hardware** page, expand the **New hard disk** pane.
   b) From the **VM storage policy** drop-down menu, select the storage policy to assign to the virtual disk.
   c) Optional: Change the storage location of the virtual disk.

      Use this option to store the virtual disk on a datastore other than the datastore where the VM configuration file resides.
4. Complete the virtual machine provisioning process.

After you create the virtual machine, the **Summary** tab displays the assigned storage policies and their compliance status. If storage placement requirements for the configuration file or the virtual disks change, you can later modify the virtual policy assignment.

Change Storage Policy Assignment for Virtual Machine Files and Disks

If your storage requirements for the applications on the virtual machine change, you can edit the storage policy that was originally applied to the virtual machine.

You can edit the storage policy for a powered-off or powered-on virtual machine.
When changing the VM storage policy assignment, you can apply the same storage policy to the virtual machine configuration file and all its virtual disks. You can also associate different storage policies with the VM configuration file

and the virtual disks. You might apply different policies when, for example, storage requirements for your virtual disks and the configuration file are different.

1. In the vSphere Client, browse to the virtual machine.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**.
   c) Click the storage policy you want to change, and click **VM Compliance**.
      You can see the list of virtual machines that use this storage policy.
   d) Click the virtual machine whose policy you want to modify.
2. Click the **Configure** tab and click **Policies**.
3. Click **Edit VM Storage Policies**.
4. Specify the VM storage policy for your virtual machine.

Option	Actions
Apply the same storage policy to all virtual machine objects	Select the policy from the **VM storage policy** drop-down menu.
Apply different storage policies to the VM home object and virtual disks	1. Turn on the **Configure per disk** option. 2. Select the object, for example, VM home. 3. In the VM Storage Policy column, select the policy from the drop-down menu.

5. If you use Virtual Volumes policy with replication, configure the replication group.
   Replication groups indicate which VMs and virtual disks must be replicated together to a target site.

   All storage objects of a VM should belong to the same replication group. You cannot assign different replication groups to different storage objects of a VM.
6. Click **OK** to save the VM storage policy changes.

The storage policy is assigned to the virtual machine and its disks.

Check Compliance for a VM Storage Policy

You can check whether a virtual machine uses a datastore that is compatible with the storage requirements specified in the VM storage policy.

Verify that the virtual machine has a storage policy that is associated with it.

1. In the vSphere Client, navigate to the virtual machine.
2. Click the **Configure** tab and click **Policies**.
3. Click **Check VM Storage Policy Compliance**.
   The system verifies the compliance.
4. View the compliance status.

Compliance Status	Description
Compliant	The datastore that the virtual machine or virtual disk uses has the storage capabilities compatible with the policy requirements.
Noncompliant	The datastore that the virtual machine or virtual disk uses does not have the storage capabilities compatible with the policy requirements. You can migrate the virtual machine files and virtual disks to compliant datastores.

Compliance Status	Description
Out of Date	The status indicates that the policy has been edited, but the new requirements have not been communicated to the datastore where the virtual machine objects reside. To communicate the changes, reapply the policy to the objects that are out of date.
Not Applicable	This storage policy references datastore capabilities that are not supported by the datastore where virtual machine resides.

When you cannot bring the noncompliant datastore into compliance, migrate the files or virtual disks to a compatible datastore. See Find Compatible Storage Resource for Noncompliant Virtual Machine.

If the status is Out of Date, reapply the policy to the objects. See Reapply Virtual Machine Storage Policy.

Find Compatible Storage Resource for Noncompliant Virtual Machine

Determine which datastore is compatible with the storage policy that is associated with your virtual machine.

Occasionally, a storage policy that is assigned to a virtual machine can be in the noncompliant status. This status indicates that the virtual machine or its disks use datastores that are incompatible with the policy. You can migrate the virtual machine files and virtual disks to compatible datastores.

Use this task to determine which datastores satisfy the requirements of the policy.

1. Verify that the storage policy for the virtual machine is in the noncompliant state.
   a) In the vSphere Client, navigate to the virtual machine.
   b) Click the **Summary** tab.
      The VM Storage Policy Compliance panel on the VM Storage Policies pane shows the Noncompliant status.
2. Navigate to the noncompliant storage policy.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**.
3. Display the list of compatible datastores for the noncompliant storage policy.
   a) Click the storage policy.
   b) Click **Storage Compatibility**.
   The list of datastores that match the requirements of the policy appears.

You can migrate the virtual machine or its disks to one of the datastores in the list.

Reapply Virtual Machine Storage Policy

After you edit a storage policy that is already associated with a virtual machine object, you must reapply the policy. By reapplying the policy, you communicate new storage requirements to the datastore where the virtual machine object resides.

The compliance status for a virtual machine is Out of Date. The status indicates that the policy has been edited, but the new requirements have not been communicated to the datastore.

1. In the vSphere Client, navigate to the virtual machine.
2. Click the **Configure** tab and click **Policies**.
3. Verify that the compliance status is Out of Date.
4. Click **Reapply VM Storage Policy**.
5. Check the compliance status.

Compliance Status	Description
Compliant	The datastore that the virtual machine or virtual disk uses has the storage capabilities that the policy requires.
Noncompliant	The datastore supports specified storage requirements, but cannot currently satisfy the storage policy. For example, the status might become Noncompliant when physical resources of the datastore are unavailable. You can bring the datastore into compliance by making changes in the physical configuration of your host cluster. For example, by adding hosts or disks to the cluster. If additional resources satisfy the storage policy, the status changes to Compliant. When you cannot bring the noncompliant datastore into compliance, migrate the files or virtual disks to a compatible datastore. See Find Compatible Storage Resource for Noncompliant Virtual Machine.
Not Applicable	The storage policy references datastore capabilities that are not supported by the datastore.

Default Storage Policies

When you provision a virtual machine on a datastore, you must assign to the virtual machine a compatible VM storage policy. If you do not configure and explicitly assign the storage policy to the virtual machine, the system uses a default storage policy.

VMware-Provided Default Storage Policy

The generic default storage policy that ESXi provides applies to all datastores and does not include rules specific to any storage type.

In addition, ESXi offers the default storage policies for object-based datastores, vSAN or Virtual Volumes. These policies guarantee the optimum placement for the virtual machine objects within the object-based storage.

For information about the default storage policy for Virtual Volumes, see Virtual Volumes and VM Storage Policies.

VMFS and NFS datastores do not have specific default policies and can use the generic default policy or a custom policy you define for them.

User-Defined Default Storage Policies

You can create a VM storage policy that is compatible with vSAN or Virtual Volumes. You can then designate this policy as the default for vSAN and Virtual Volumes datastores. The user-defined default policy replaces the default storage policy that VMware provides.

Each vSAN and Virtual Volumes datastore can have only one default policy at a time. However, you can create a single storage

policy with multiple placement rule sets, so that it matches multiple vSAN and Virtual Volumes datastores. You can designate this policy as the default policy for all datastores.

When the VM storage policy becomes the default policy for a datastore, you cannot delete the policy unless you disassociate it from the datastore.

Change the Default Storage Policy for a Datastore

For Virtual Volumes and vSAN datastores, VMware provides storage policies that are used as the default during the virtual machine provisioning. You can change the default storage policy for a selected Virtual Volumes or vSAN datastore.

Create a storage policy that is compatible with Virtual Volumes or vSAN. You can create a policy that matches both types of storage.

Note: Do not designate a storage policy with replication rules as a default storage policy. Otherwise, the policy prevents you from selecting replication groups.

1. In the vSphere Client, navigate to the datastore.
2. Click the **Configure** tab, and click **General**.
3. In the Default Storage Policy pane, click **Edit**.
4. From the list of available storage policies, select a policy to designate as the default and click **OK**.

The selected storage policy becomes the default policy for the datastore. The system assigns this policy to any virtual machine objects that you provision on the datastore when no other policy is selected.

Using Storage Providers

A storage provider is a software component that is offered by VMware or developed by a third party through vSphere APIs for Storage Awareness (VASA). The storage provider can also be called VASA provider. The storage providers integrate with various storage entities that include external physical storage and storage abstractions, such as vSAN and Virtual Volumes. Storage providers can also support software solutions, for example, I/O filters.

About Storage Providers

Generally, vCenter Server and ESXi use the storage providers to obtain information about storage configuration, status, and storage data services offered in your environment. This information appears in the vSphere Client. The information helps you to make appropriate decisions about virtual machine placement, to set storage requirements, and to monitor your storage environment.

Persistence Storage Providers
Storage providers that manage arrays and storage abstractions, are called persistence storage providers. Providers that support Virtual Volumes or vSAN belong to this category. In addition to storage, persistence providers can provide other data services, such as replication.

Data Service Providers
Another category of providers is I/O filter storage providers, or data service providers. These providers offer data services that include host-based caching, compression, and encryption.

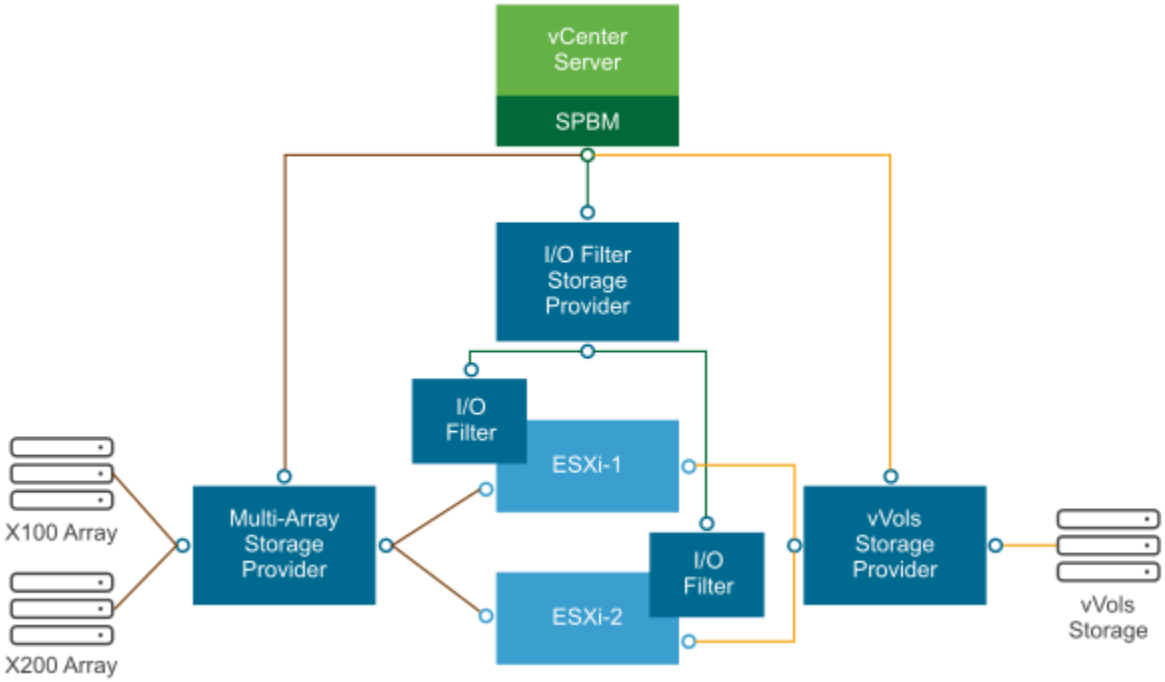
Both persistence storage and data service providers can belong to one of these categories.

Built-in Storage Providers
Built-in storage providers are offered by VMware. Typically, they do not require registration. For example, the storage providers that support vSAN or I/O filters are build-in and become registered automatically.

Third-Party Storage Providers

When a third party offers a storage provider, you typically must register the provider. An example of such a provider is the Virtual Volumes provider. You use the vSphere Client to register and manage each storage provider component.

The following graphic illustrates how different types of storage providers facilitate communications between vCenter Server and ESXi and other components of your storage environment. For example, the components might include storage arrays, Virtual Volumes storage, and I/O filters.



Storage Providers and Data Representation

vCenter Server and ESXi communicate with the storage provider to obtain information that the storage provider collects from underlying physical and software-defined storage, or from available I/O filters. vCenter Server can then display the storage data in the vSphere Client.

Information that the storage provider supplies can be divided into the following categories:

- Storage data services and capabilities. This type of information is essential for such functionalities as vSAN, Virtual Volumes, and I/O filters. The storage provider that represents these functionalities integrates with the Storage Policy Based Management (SPBM) mechanism. The storage provider collects information about data services that are offered by underlying storage entities or available I/O filters.

  You reference these data services when you define storage requirements for virtual machines and virtual disks in a storage policy. Depending on your environment, the SPBM mechanism ensures appropriate storage placement for a virtual machine or enables specific data services for virtual disks. For details, see Creating and Managing VM Storage Policies.

- Storage status. This category includes reporting about status of various storage entities. It also includes alarms and events for notifying about configuration changes.
  This type of information can help you troubleshoot storage connectivity and performance problems. It can also help you to correlate array-generated events and alarms to corresponding performance and load changes on the array.
- Storage DRS information for the distributed resource scheduling on block devices or file systems. This information helps to ensure that decisions made by Storage DRS are compatible with resource management decisions internal to the storage systems.

Storage Provider Requirements and Considerations

When you use the third-party storage providers, certain requirements and considerations apply.

Typically, vendors are responsible for supplying storage providers. The VMware VASA program defines an architecture that integrates third-party storage providers into the vSphere environment, so that vCenter Server and ESXi hosts can communicate with the storage providers.

To use storage providers, follow these requirements:

- Make sure that every storage provider you use is certified by VMware and properly deployed. For information about deploying the storage providers, contact your storage vendor.
- Make sure that the storage provider is compatible with the vCenter Server and ESXi versions. See *VMware Compatibility Guide*.
- Do not install the VASA provider on the same system as vCenter Server.
- If your environment contains older versions of storage providers, existing functionality continues to work. However, to use new features, upgrade your storage provider to a new version.
- When you upgrade a storage provider to a later VASA version, you must unregister and reregister the provider. After registration, vCenter Server can detect and use the functionality of the new VASA version.

Register Storage Providers

To establish a connection between vCenter Server and a storage provider, you must register the storage provider. Use the vSphere Client to register a separate storage provider for each host in a cluster.

Verify that the storage provider component is installed on the storage side and obtain its credentials from your storage administrator.

When you upgrade a storage provider to a later VASA version, you must unregister and reregister the provider. After registration, vCenter Server can detect and use the functionality of the later VASA version.
Note: If you use vSAN, the storage providers for vSAN are registered and appear on the list of storage providers automatically. vSAN does not support manual registration of storage providers. See the *Administering VMware vSAN* documentation.

1. Navigate to vCenter Server.
2. Click the **Configure** tab, and click **Storage Providers**.
3. Click the **Add** icon.
4. Enter connection information for the storage provider, including the name, URL, and credentials.
5. Specify the security method.

Action	Description
Direct vCenter Server to the storage provider certificate	Select the **Use storage provider certificate** option and specify the certificate's location.
Use a thumbprint of the storage provider certificate	If you do not guide vCenter Server to the provider certificate, the certificate thumbprint is displayed. You can check the

Action	Description
	thumbprint and approve it. vCenter Server adds the certificate to the truststore and proceeds with the connection.

The storage provider adds the vCenter Server certificate to its truststore when vCenter Server first connects to the provider.

6. Click **OK**.

vCenter Server registers the storage provider and establishes a secure SSL connection with it.

View Storage Provider Information

After you register a storage provider component with vCenter Server, the storage provider appears on the storage providers list. Certain storage providers are self-registered and automatically appear on the list after you set up the entity they represent, for example, vSAN or I/O filters.

Use the vSphere Client to view general storage provider information and details for each storage component.

1. Navigate to vCenter Server.
2. Click the **Configure** tab, and click **Storage Providers**.
3. In the Storage Providers list, view the storage providers registered with vCenter Server.

   The list shows general information including the name of the storage provider, its URL and status, version of VASA APIs, storage entities the provider represents, and so on.
4. To display additional details, select a specific storage provider or its component from the list.

   Note: A single storage provider can support storage systems from multiple different vendors.

Manage Storage Providers

Use the vSphere Client to perform several management operations on the registered storage providers.

1. Navigate to vCenter Server.
2. Click the **Configure** tab, and click **Storage Providers**.
3. From the list of storage providers, select a storage provider and click one of the following icons.

Option	Description
Synchronize Storage Providers	Synchronize all storage providers with the current state of the environment.
Rescan	Update storage data for the provider. vCenter Server periodically updates storage data in its database. The updates are partial and reflect only those changes that storage providers communicate to vCenter Server at that moment. When needed, you can perform a full database synchronization for the selected storage provider.
Remove	Unregister storage providers that you do not use. After this operation, vCenter Server closes the connection and removes the storage provider from its configuration. **Note:** You cannot manually unregister certain storage providers supplied by VMware, for example, vSAN storage providers. This option is also useful when you upgrade a storage provider to a later VASA version. In this case, you must unregister and

Option	Description
	then reregister the provider. After registration, vCenter Server can detect and use the functionality of the later VASA version.
Refresh certificate	vCenter Server warns you when a certificate assigned to a storage provider is about to expire. You can refresh the certificate to continue using the provider. If you fail to refresh the certificate before it expires, vCenter Server discontinues using the provider.

vCenter Server closes the connection and removes the storage provider from its configuration.

Working with VMware vSphere Virtual Volumes

VMware vSphere Virtual Volumes, also known as vVols, virtualizes SAN and NAS devices by abstracting physical hardware resources into logical pools of capacity. The Virtual Volumes functionality changes the storage management paradigm from managing space inside datastores to managing abstract storage objects handled by storage arrays.

About Virtual Volumes

With Virtual Volumes, an individual virtual machine, not the datastore, becomes a unit of storage management, while storage hardware gains complete control over virtual disk content, layout, and management.

Historically, vSphere storage management used a datastore-centric approach. With this approach, storage administrators and vSphere administrators discuss in advance the underlying storage requirements for virtual machines. The storage administrator then sets up LUNs or NFS shares and presents them to ESXi hosts. The vSphere administrator creates datastores based on LUNs or NFS, and uses these datastores as virtual machine storage. Typically, the datastore is the lowest granularity level at which data management occurs from a storage perspective. However, a single datastore contains multiple virtual machines, which might have different requirements. With the traditional approach, it is difficult to meet the requirements of an individual virtual machine.

The Virtual Volumes functionality helps to improve granularity. It helps you to differentiate virtual machine services on a per application level by offering a new approach to storage management. Rather than arranging storage around features of a storage system, Virtual Volumes arranges storage around the needs of individual virtual machines, making storage virtual-machine centric.

Virtual Volumes maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. This mapping allows vSphere to offload intensive storage operations such as snapshot, cloning, and replication to the storage system.

By creating a volume for each virtual disk, you can set policies at the optimum level. You can decide in advance what the storage requirements of an application are, and communicate these requirements to the storage system. The storage system creates an appropriate virtual disk based on these requirements. For example, if your virtual machine requires an active-active storage array, you no longer must select a datastore that supports the active-active model. Instead, you create an individual virtual volume that is automatically placed to the active-active array.

Virtual Volumes Concepts

With Virtual Volumes, abstract storage containers replace traditional storage volumes based on LUNs or NFS shares. In vCenter Server, the storage containers are represented by Virtual Volumes datastores. Virtual Volumes datastores store virtual volumes, objects that encapsulate virtual machine files.

Watch the video to learn more about different components of the Virtual Volumes functionality.

Virtual Volume Objects

Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual volumes are stored natively inside a storage system that is connected to your ESXi hosts through Ethernet or SAN. They are exported as objects by a compliant storage system and are managed entirely by hardware on the storage side. Typically, a unique GUID identifies a virtual volume. Virtual volumes are not preprovisioned, but created automatically when you perform virtual machine management operations. These operations include a VM creation, cloning, and snapshotting. ESXi and vCenter Server associate one or more virtual volumes to a virtual machine.

Types of Virtual Volumes

The system creates the following types of virtual volumes for the core elements that make up the virtual machine:

Data-vVol	A data virtual volume that corresponds directly to each virtual disk `.vmdk` file. As virtual disk files on traditional datastores, virtual volumes are presented to virtual machines as SCSI disks. Data-vVol can be either thick or thin-provisioned.
Config-vVol	A configuration virtual volume, or a home directory, represents a small directory that contains metadata files for a virtual machine. The files include a `.vmx` file, descriptor files for virtual disks, log files, and so forth. The configuration virtual volume is formatted with a file system. When ESXi uses the SCSI protocol to connect to storage, configuration virtual volumes are formatted with VMFS. With NFS protocol, configuration virtual volumes are presented as an NFS directory. Typically, it is thin-provisioned. **Note:** Starting with vSphere 7.0 Update 2, partners can increase the config-vVol to above 4 GB. Work with your Virtual Volumes partner on implementing this if it is supported by your partner and applicable to your environment.
Swap-vVol	Created when a VM is first powered on. It is a virtual volume to hold copies of VM memory pages that cannot be retained in memory. Its size is determined by the VM's memory size. It is thick-provisioned by default.
Snapshot-vVol	A virtual memory volume to hold the contents of virtual machine memory for a snapshot. Thick-provisioned.
Other	A virtual volume for specific features. For example, a digest virtual volume is created for Content-Based Read Cache (CBRC).

Typically, a VM creates a minimum of three virtual volumes, data-vVol, config-vVol, and swap-vVol. The maximum depends on how many virtual disks and snapshots reside on the VM.

For example, the following SQL server has six virtual volumes:

- Config-vVol
- Data-vVol for the operating system
- Data-vVol for the database
- Data-vVol for the log
- Swap-vVol when powered on
- Snapshot-vVol

By using different virtual volumes for different VM components, you can apply and manipulate storage policies at the finest granularity level. For example, a virtual volume that contains a virtual disk can have a richer set of services than the virtual volume for the VM boot disk. Similarly, a snapshot virtual volume can use a different storage tier compared to a current virtual volume.

Disk Provisioning

The Virtual Volumes functionality supports a concept of thin and thick-provisioned virtual disks. However, from the I/O prospective, implementation and management of thin or thick provisioning by the arrays is transparent to the ESXi host. ESXi offloads to the storage arrays any functions related to thin provisioning. In the data path, ESXi does not treat the thin or thick virtual volumes differently.

You select the thin or thick type for your virtual disk at the VM creation time. If your disk is thin and resides on a Virtual Volumes datastore, you cannot change its type later by inflating the disk.

Shared Disks

You can place a shared disk on a Virtual Volumes storage that supports SCSI Persistent Reservations for Virtual Volumes. You can use this disk as a quorum disk and eliminate RDMs in the MSCS clusters. For more information, see the *vSphere Resource Management* documentation.

Related Links

Virtual Volumes Storage Providers on page 2605
A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

Virtual Volumes Storage Containers on page 2606
Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

Protocol Endpoints on page 2607
Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Binding and Unbinding Virtual Volumes to Protocol Endpoints on page 2608
At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

Virtual Volumes Datastores on page 2609
A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

Virtual Volumes and VM Storage Policies on page 2610
A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

Virtual Volumes Storage Providers

A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

The storage provider is implemented through VMware APIs for Storage Awareness (VASA) and is used to manage all aspects of Virtual Volumes storage. The storage provider integrates with the Storage Monitoring Service (SMS), shipped with vSphere, to communicate with vCenter Server and ESXi hosts.

The storage provider delivers information from the underlying storage container. The storage container capabilities appear in vCenter Server and the vSphere Client. Then, in turn, the storage provider communicates virtual machine storage requirements, which you can define in the form of a storage policy, to the storage layer. This integration process ensures that a virtual volume created in the storage layer meets the requirements outlined in the policy.

Typically, vendors are responsible for supplying storage providers that can integrate with vSphere and provide support to Virtual Volumes. Every storage provider must be certified by VMware and properly deployed. For information about deploying and upgrading the Virtual Volumes storage provider to a version compatible with current ESXi release, contact your storage vendor.

After you deploy the storage provider, you must register it in vCenter Server, so that it can communicate with vSphere through the SMS.

Related Links

Virtual Volume Objects on page 2604
Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual Volumes Storage Containers on page 2606
Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

Protocol Endpoints on page 2607
Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Binding and Unbinding Virtual Volumes to Protocol Endpoints on page 2608
At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

Virtual Volumes Datastores on page 2609
A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

Virtual Volumes and VM Storage Policies on page 2610
A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

Virtual Volumes Storage Containers

Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

A storage container is a part of the logical storage fabric and is a logical unit of the underlying hardware. The storage container logically groups virtual volumes based on management and administrative needs. For example, the storage container can contain all virtual volumes created for a tenant in a multitenant deployment, or a department in an enterprise deployment. Each storage container serves as a virtual volume store and virtual volumes are allocated out of the storage container capacity.

Typically, a storage administrator on the storage side defines storage containers. The number of storage containers, their capacity, and their size depend on a vendor-specific implementation. At least one container for each storage system is required.

Note: A single storage container cannot span different physical arrays.

After you register a storage provider associated with the storage system, vCenter Server discovers all configured storage containers along with their storage capability profiles, protocol endpoints, and other attributes. A single storage container can export multiple capability profiles. As a result, virtual machines with diverse needs and different storage policy settings can be a part of the same storage container.

Initially, all discovered storage containers are not connected to any specific host, and you cannot see them in the vSphere Client. To mount a storage container, you must map it to a Virtual Volumes datastore.

Related Links

Virtual Volume Objects on page 2604
Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual Volumes Storage Providers on page 2605
A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

Protocol Endpoints on page 2607
Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Binding and Unbinding Virtual Volumes to Protocol Endpoints on page 2608
At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

Virtual Volumes Datastores on page 2609
A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

Virtual Volumes and VM Storage Policies on page 2610
A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

Protocol Endpoints

Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Each virtual volume is bound to a specific protocol endpoint. When a virtual machine on the host performs an I/O operation, the protocol endpoint directs the I/O to the appropriate virtual volume. Typically, a storage system requires just a few protocol endpoints. A single protocol endpoint can connect to hundreds or thousands of virtual volumes.

On the storage side, a storage administrator configures protocol endpoints, one or several per storage container. The protocol endpoints are a part of the physical storage fabric. The storage system exports the protocol endpoints with associated storage containers through the storage provider. After you map the storage container to a Virtual Volumes datastore, the ESXi host discovers the protocol endpoints and they become visible in the vSphere Client. The protocol endpoints can also be discovered during a storage rescan. Multiple hosts can discover and mount the protocol endpoints.

In the vSphere Client, the list of available protocol endpoints looks similar to the host storage devices list. Different storage transports can be used to expose the protocol endpoints to ESXi. When the SCSI-based transport is used, the protocol endpoint represents a proxy LUN defined by a T10-based LUN WWN. For the NFS protocol, the protocol endpoint is a mount point, such as an IP address and a share name. You can configure multipathing on the SCSI-based protocol endpoint, but not on the NFS-based protocol endpoint. No matter which protocol you use, the storage array can provide multiple protocol endpoints for availability purposes.

Protocol endpoints are managed per array. ESXi and vCenter Server assume that all protocol endpoints reported for an array are associated with all containers on that array. For example, if an array has two containers and three protocol endpoints, ESXi assumes that virtual volumes on both containers can be bound to all three protocol points.

Related Links

Virtual Volume Objects on page 2604
Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual Volumes Storage Providers on page 2605
A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

Virtual Volumes Storage Containers on page 2606
Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

Binding and Unbinding Virtual Volumes to Protocol Endpoints on page 2608
At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

Virtual Volumes Datastores on page 2609
A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

Virtual Volumes and VM Storage Policies on page 2610
A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

Binding and Unbinding Virtual Volumes to Protocol Endpoints

At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

The storage system replies with a protocol endpoint ID that becomes an access point to the virtual volume. The protocol endpoint accepts all I/O requests to the virtual volume. This binding exists until ESXi sends an unbind request for the virtual volume.

For later bind requests on the same virtual volume, the storage system can return different protocol endpoint IDs.

When receiving concurrent bind requests to a virtual volume from multiple ESXi hosts, the storage system can return the same or different endpoint bindings to each requesting ESXi host. In other words, the storage system can bind different concurrent hosts to the same virtual volume through different endpoints.

The unbind operation removes the I/O access point for the virtual volume. The storage system might unbind the virtual volume from its protocol endpoint immediately, or after a delay, or take some other action. A bound virtual volume cannot be deleted until it is unbound.

Related Links

Virtual Volume Objects on page 2604
Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual Volumes Storage Providers on page 2605
A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

Virtual Volumes Storage Containers on page 2606
Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

Protocol Endpoints on page 2607
Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Virtual Volumes Datastores on page 2609
A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

Virtual Volumes and VM Storage Policies on page 2610
A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

Virtual Volumes Datastores

A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

After vCenter Server discovers storage containers exported by storage systems, you must mount them as Virtual Volumes datastores. The Virtual Volumes datastores are not formatted in a traditional way like, for example, VMFS datastores. You must still create them because all vSphere functionalities, including FT, HA, DRS, and so on, require the datastore construct to function properly.

You use the datastore creation wizard in the vSphere Client to map a storage container to a Virtual Volumes datastore. The Virtual Volumes datastore that you create corresponds directly to the specific storage container.

From a vSphere administrator prospective, the Virtual Volumes datastore is similar to any other datastore and is used to hold virtual machines. Like other datastores, the Virtual Volumes datastore can be browsed and lists virtual volumes by virtual machine name. Like traditional datastores, the Virtual Volumes datastore supports unmounting and mounting. However, such operations as upgrade and resize are not applicable to the Virtual Volumes datastore. The Virtual Volumes datastore capacity is configurable by the storage administrator outside of vSphere.

You can use the Virtual Volumes datastores with traditional VMFS and NFS datastores and with vSAN.

Note: The size of a virtual volume must be a multiple of 1 MB, with a minimum size of 1 MB. As a result, all virtual disks that you provision on a Virtual Volumes datastore must be an even multiple of 1 MB. If the virtual disk you migrate to the Virtual Volumes datastore is not an even multiple of 1 MB, extend the disk to the nearest even multiple of 1 MB.

Related Links

Virtual Volume Objects on page 2604
Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual Volumes Storage Providers on page 2605
A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

Virtual Volumes Storage Containers on page 2606
Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

Protocol Endpoints on page 2607
Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Binding and Unbinding Virtual Volumes to Protocol Endpoints on page 2608
At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

Virtual Volumes and VM Storage Policies on page 2610
A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

Virtual Volumes and VM Storage Policies

A virtual machine that runs on a Virtual Volumes datastore requires a VM storage policy.

A VM storage policy is a set of rules that contains placement and quality-of-service requirements for a virtual machine. The policy enforces appropriate placement of the virtual machine within Virtual Volumes storage and guarantees that storage can satisfy virtual machine requirements.

You use the VM Storage Policies interface to create a Virtual Volumes storage policy. When you assign the new policy to the virtual machine, the policy enforces that the Virtual Volumes storage meets the requirements.

Virtual Volumes Default Storage Policy

For Virtual Volumes, VMware provides a default storage policy that contains no rules or storage requirements, called Virtual Volumes No Requirements Policy. This policy is applied to the VM objects when you do not specify another policy for the virtual machine on the Virtual Volumes datastore. With the No Requirements policy, storage arrays can determine the optimum placement for the VM objects.

The default No Requirements policy that VMware provides has the following characteristics:

- You cannot delete, edit, or clone this policy.
- The policy is compatible only with the Virtual Volumes datastores.
- You can create a VM storage policy for Virtual Volumes and designate it as the default.

Related Links

Virtual Volume Objects on page 2604
Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives.

Virtual Volumes Storage Providers on page 2605
A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other.

Virtual Volumes Storage Containers on page 2606
Unlike traditional LUN and NFS-based storage, the Virtual Volumes functionality does not require preconfigured volumes on a storage side. Instead, Virtual Volumes uses a storage container. It is a pool of raw storage capacity or an aggregation of storage capabilities that a storage system can provide to virtual volumes.

Protocol Endpoints on page 2607
Although storage systems manage all aspects of virtual volumes, ESXi hosts have no direct access to virtual volumes on the storage side. Instead, ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

Binding and Unbinding Virtual Volumes to Protocol Endpoints on page 2608
At the time of creation, a virtual volume is a passive entity and is not immediately ready for I/O. To access the virtual volume, ESXi or vCenter Server send a bind request.

Virtual Volumes Datastores on page 2609
A Virtual Volumes datastore represents a storage container in vCenter Server and the vSphere Client.

Virtual Volumes and Storage Protocols

A Virtual Volumes storage system provides protocol endpoints that are discoverable on the physical storage fabric. ESXi hosts use the protocol endpoints to connect to virtual volumes on the storage. Operation of the protocol endpoints depends on storage protocols that expose the endpoints to ESXi hosts.

Virtual Volumes supports NFS version 3 and 4.1, iSCSI, Fibre Channel, and FCoE.

No matter which storage protocol is used, protocol endpoints provide uniform access to both SAN and NAS storage. A virtual volume, like a file on other traditional datastore, is presented to a virtual machine as a SCSI disk.

Note: A storage container is dedicated to SCSI or NAS and cannot be shared across those protocol types. An array can present one storage container with SCSI protocol endpoints and a different container with NFS protocol endpoints. The container cannot use a combination of SCSI and NFS protocol endpoints.

Virtual Volumes and SCSI-Based Transports

On disk arrays, Virtual Volumes supports Fibre Channel, FCoE, and iSCSI protocols.

When the SCSI-based protocol is used, the protocol endpoint represents a proxy LUN defined by a T10-based LUN WWN.

As any block-based LUNs, the protocol endpoints are discovered using standard LUN discovery commands. The ESXi host periodically rescans for new devices and asynchronously discovers block-based protocol endpoints. The protocol endpoint can be accessible by multiple paths. Traffic on these paths follows well-known path selection policies, as is typical for LUNs.

On SCSI-based disk arrays at VM creation time, ESXi makes a virtual volume and formats it as VMFS. This small virtual volume stores all VM metadata files and is called the config-vVol. The config-vVol functions as a VM storage locator for vSphere.

Virtual Volumes on disk arrays supports the same set of SCSI commands as VMFS and use ATS as a locking mechanism.

CHAP Support for iSCSI Endpoints

Virtual Volumes supports Challenge Handshake Access Protocol (CHAP) with iSCSI targets. This support allows ESXi hosts to share CHAP initiator credentials with Virtual Volumes storage providers, also called VASA providers, and for Virtual Volumes storage providers to raise system events notifying vCenter Server of changes to CHAP target credentials on the storage array.

Each ESXi host can have multiple HBAs and each HBA can have properties configured on it. One of these properties is the authentication method that the HBA must use. Authentication is optional, but if implemented, it must be supported by both the initiator and target. CHAP is an authentication method that can be used both directions between initiator and target.

For more information about different CHAP authentication methods, see Selecting CHAP Authentication Method. To configure CHAP on your ESXi host, see Configuring CHAP Parameters for iSCSI or iSER Storage Adapters.

Virtual Volumes and NFS Transports

With NAS storage, a protocol endpoint is an NFS share that the ESXi host mounts using IP address or DNS name and a share name. Virtual Volumes supports NFS version 3 and 4.1 to access NAS storage. Both IPv4 and IPv6 formats are supported.

No matter which version you use, a storage array can provide multiple protocol endpoints for availability purposes.

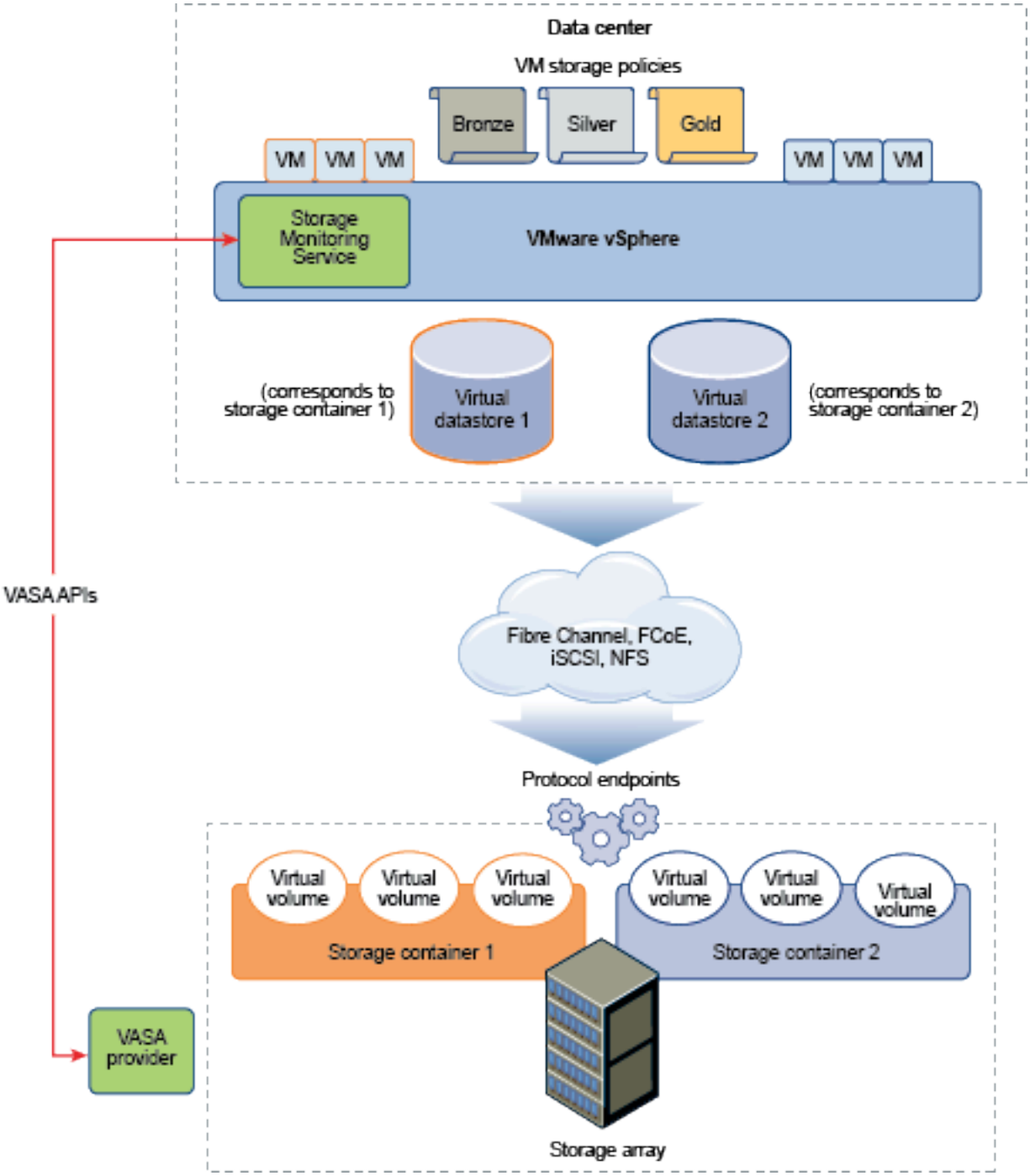
In addition, NFS version 4.1 introduces trunking mechanisms that enable load balancing and multipathing.

Virtual Volumes on NAS devices supports the same NFS Remote Procedure Calls (RPCs) that ESXi hosts use when connecting to NFS mount points.

On NAS devices, a config-vVol is a directory subtree that corresponds to a config-vVolID. The config-vVol must support directories and other operations that are necessary for NFS.

Virtual Volumes Architecture

An architectural diagram provides an overview of how all components of the Virtual Volumes functionality interact with each other.



Virtual volumes are objects exported by a compliant storage system and typically correspond one-to-one with a virtual machine disk and other VM-related files. A virtual volume is created and manipulated out-of-band, not in the data path, by a VASA provider.

A VASA provider, or a storage provider, is developed through vSphere APIs for Storage Awareness. The storage provider enables communication between the ESXi hosts, vCenter Server, and the vSphere Client on one side, and the storage system on the other. The VASA provider runs on the storage side and integrates with the vSphere Storage Monitoring Service (SMS) to manage all aspects of Virtual Volumes storage. The VASA provider maps virtual disk objects and their derivatives, such as clones, snapshots, and replicas, directly to the virtual volumes on the storage system.

The ESXi hosts have no direct access to the virtual volumes storage. Instead, the hosts access the virtual volumes through an intermediate point in the data path, called the protocol endpoint. The protocol endpoints establish a data path on demand from the virtual machines to their respective virtual volumes. The protocol endpoints serve as a gateway for direct in-band I/O between ESXi hosts and the storage system. ESXi can use Fibre Channel, FCoE, iSCSI, and NFS protocols for in-band communication.

The virtual volumes reside inside storage containers that logically represent a pool of physical disks on the storage system. On the vCenter Server and ESXi side, storage containers are presented as Virtual Volumes datastores. A single storage container can export multiple storage capability sets and provide different levels of service to different virtual volumes.

Watch the video for information about Virtual Volumes architecture.

Virtual Volumes and VMware Certificate Authority

vSphere includes the VMware Certificate Authority (VMCA). By default, the VMCA creates all internal certificates used in vSphere environment. It generates certificates for newly added ESXi hosts and storage VASA providers that manage or represent Virtual Volumes storage systems.

Communication with the VASA provider is protected by SSL certificates. These certificates can come from the VASA provider or from the VMCA.

- Certificates can be directly provided by the VASA provider for long-term use. They can be either self-generated and self-signed, or derived from an external Certificate Authority.
- Certificates can be generated by the VMCA for use by the VASA provider.

When a host or VASA provider is registered, VMCA follows these steps automatically, without involvement from the vSphere administrator.

1. When a VASA provider is first added to the vCenter Server storage management service (SMS), it produces a self-signed certificate.
2. After verifying the certificate, the SMS requests a Certificate Signing Request (CSR) from the VASA provider.
3. After receiving and validating the CSR, the SMS presents it to the VMCA on behalf of the VASA provider, requesting a CA signed certificate.

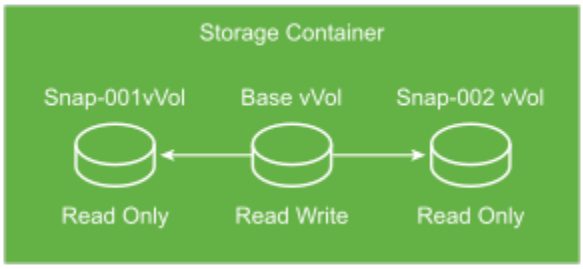
   The VMCA can be configured to function as a standalone CA, or as a subordinate to an enterprise CA. If you set up the VMCA as a subordinate CA, the VMCA signs the CSR with the full chain.
4. The signed certificate with the root certificate is passed to the VASA provider. The VASA provider can authenticate all future secure connections originating from the SMS on vCenter Server and on ESXi hosts.

Virtual Volume Snapshots

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines. Virtual volumes snapshots serve many purposes. You can use them to create a quiesced copy for backup or archival purposes, or to create a test and rollback environment for applications. You can also use them to provision application images instantly.

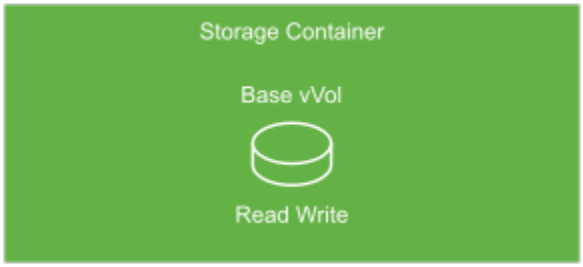
In Virtual Volumes environment, snapshots are managed by ESXi and vCenter Server, but are performed by the storage array.

Each snapshot creates an extra virtual volume object, a snapshot virtual volume, that holds the contents of virtual machine memory. Original VM data is copied to this object, and it remains read-only, which prevents the guest operating system from writing to snapshot. You cannot resize the snapshot virtual volume. Typically, when you replicate the VM, its snapshot virtual volume is also replicated.



The base virtual volume remains active, or read-write. When another snapshot is created, it preserves the new state and data of the virtual machine at the time you take the snapshot.

When you delete snapshots, only the base virtual volume remains, while snapshot virtual volume objects are discarded. The base virtual volume represents the most current state of the virtual machine. Unlike snapshots on the traditional datastores, snapshot virtual volumes do not need to commit their contents to the base virtual volume.



For information about creating and managing snapshots, see the *vSphere Virtual Machine Administration* documentation.

Before You Enable Virtual Volumes

To work with Virtual Volumes, you must make sure that your storage and vSphere environment are set up correctly.

Prepare Storage System for Virtual Volumes

To prepare your storage system environment for Virtual Volumes, follow these guidelines. For additional information, contact your storage vendor.

- The storage system or storage array that you use must support Virtual Volumes and integrate with the vSphere components through vSphere APIs for Storage Awareness (VASA). The storage array must support thin provisioning and snapshotting.
- The Virtual Volumes storage provider must be deployed.
- The following components must be configured on the storage side:
  - Protocol endpoints
  - Storage containers
  - Storage profiles
  - Replication configurations if you plan to use Virtual Volumes with replication. See Requirements for Replication with Virtual Volumes.

Prepare vSphere Environment

- Make sure to follow appropriate setup guidelines for the type of storage you use, Fibre Channel, FCoE, iSCSI, or NFS. If necessary, install and configure storage adapters on your ESXi hosts.
  - If you use iSCSI, activate the software iSCSI adapters on your ESXi hosts. Configure Dynamic Discovery and enter the IP address of your Virtual Volumes storage system. See Configure the Software iSCSI Adapter.
- Synchronize all components in the storage array with vCenter Server and all ESXi hosts. Use Network Time Protocol (NTP) to do this synchronization.

For more information, contact your vendor and see *VMware Compatibility Guide*

Synchronize vSphere Storage Environment with a Network Time Server

If you use Virtual Volumes, configure Network Time Protocol (NTP) to make sure all ESXi hosts on the vSphere network are synchronized.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, select **Time Configuration**.
4. Click **Edit** and set up the NTP server.
   a) Select **Use Network Time Protocol (Enable NTP client)**.
   b) Set the NTP Service Startup Policy.
   c) Enter the IP addresses of the NTP server to synchronize with.
   d) Click **Start** or **Restart** in the NTP Service Status section.
5. Click **OK**.
   The host synchronizes with the NTP server.

Configure Virtual Volumes

To configure your Virtual Volumes environment, follow several steps.

Follow guidelines in Before You Enable Virtual Volumes.

1. Register Storage Providers for Virtual Volumes.
2. Create a Virtual Volumes Datastore.
3. Review and Manage Protocol Endpoints.
4. Change the Path Selection Policy for a Protocol Endpoint.

After deploying Virtual Volumes, you can provision virtual machines on the Virtual Volumes datastore. For information on creating virtual machines, see Provision Virtual Machines on Virtual Volumes Datastores and the *vSphere Virtual Machine Administration* documentation.

Register Storage Providers for Virtual Volumes

Your Virtual Volumes environment must include storage providers, also called VASA providers. Typically, third-party vendors develop storage providers through the VMware APIs for Storage Awareness (VASA). Storage providers facilitate communication between vSphere and the storage side. Use the vSphere Client to register the Virtual Volumes storage providers.

Verify that an appropriate version of the Virtual Volumes storage provider is installed on the storage side. Obtain credentials of the storage provider.

After registration, the Virtual Volumes provider communicates with vCenter Server. The provider reports characteristics of underlying storage and data services, such as replication, that the storage system provides. The characteristics appear in the VM Storage Policies interface and can be used to create a VM storage policy compatible with the Virtual Volumes datastore. After you apply this storage policy to a virtual machine, the policy is pushed to Virtual Volumes storage. The policy enforces optimal placement of the virtual machine within Virtual Volumes storage and guarantees that storage can satisfy virtual machine requirements. If your storage provides extra services, such as caching or replication, the policy enables these services for the virtual machine.

1. Navigate to vCenter Server.
2. Click the **Configure** tab, and click **Storage Providers**.
3. Click the **Add** icon.
4. Enter connection information for the storage provider, including the name, URL, and credentials.
5. Specify the security method.

Action	Description
Direct vCenter Server to the storage provider certificate	Select the **Use storage provider certificate** option and specify the certificate's location.
Use a thumbprint of the storage provider certificate	If you do not guide vCenter Server to the provider certificate, the certificate thumbprint is displayed. You can check the thumbprint and approve it. vCenter Server adds the certificate to the truststore and proceeds with the connection.

   The storage provider adds the vCenter Server certificate to its truststore when vCenter Server first connects to the provider.

6. To complete the registration, click **OK**.

vCenter Server discovers and registers the Virtual Volumes storage provider.

Create a Virtual Volumes Datastore

You use the **New Datastore** wizard to create a Virtual Volumes datastore.

1. In the vSphere Client object navigator, browse to a host, a cluster, or a data center.
2. From the right-click menu, select **Storage** > **New Datastore**.
3. Select **vVol** as the datastore type.
4. Enter the datastore name and select a backing storage container from the list of storage containers.
   Make sure to use the name that does not duplicate another datastore name in your data center environment.

   If you mount the same Virtual Volumes datastore to several hosts, the name of the datastore must be consistent across all hosts.
5. Select the hosts that require access to the datastore.
6. Review the configuration options and click **Finish**.

After you create the Virtual Volumes datastore, you can perform such datastore operations as renaming the datastore, browsing datastore files, unmounting the datastore, and so on.

You cannot add the Virtual Volumes datastore to a datastore cluster.

Review and Manage Protocol Endpoints

ESXi hosts use a logical I/O proxy, called protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. Protocol endpoints are exported, along with associated storage containers, by the storage system through a storage provider. Protocol endpoints become visible in the vSphere Client after you map a storage container to a Virtual Volumes datastore. You can review properties of protocol endpoints and modify specific settings.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Protocol Endpoints**.
4. To view details for a specific item, select this item from the list.
5. Use tabs under Protocol Endpoint Details to access additional information and modify properties for the selected protocol endpoint.

Tab	Description
Properties	View the item properties and characteristics. For SCSI (block) items, view and edit multipathing policies.
Paths (SCSI protocol endpoints only)	Display paths available for the protocol endpoint. Disable or enable a selected path. Change the Path Selection Policy.
Datastores	Display a corresponding Virtual Volumes datastore. Perform datastore management operations.

Change the Path Selection Policy for a Protocol Endpoint

If your ESXi host uses SCSI-based transport to communicate with protocol endpoints representing a storage array, you can modify default multipathing policies assigned to protocol endpoints. Use the **Edit Multipathing Policies** dialog box to change a path selection policy.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **Storage**, click **Protocol Endpoints**.
4. Select the protocol endpoint whose paths you want to change and click the **Properties** tab.
5. Under Multipathing Policies, select **Edit Multipathing** from the **Actions** menu.
6. Select a path policy and configure its settings. Your options change depending on the type of a storage device you use.

   The path policies available for your selection depend on the storage vendor support.

   - For information about path policies for SCSI devices, see Path Selection Plug-Ins and Policies.
   - For information about path mechanisms for NVMe devices, see VMware High Performance Plug-In and Path Selection Schemes.
7. To save your settings and exit the dialog box, click **OK**.

Provision Virtual Machines on Virtual Volumes Datastores

You can provision virtual machines on a Virtual Volumes datastore.

Note: All virtual disks that you provision on a Virtual Volumes datastore must be an even multiple of 1 MB.

A virtual machine that runs on a Virtual Volumes datastore requires an appropriate VM storage policy.

After you provision the virtual machine, you can perform typical VM management tasks. For information, see the *vSphere Virtual Machine Administration* documentation.

1. Define a VM storage policy for Virtual Volumes.

   VMware provides a default No Requirements storage policy for Virtual Volumes. If you need, you can create a custom storage policy compatible with Virtual Volumes.

   See Create a VM Storage Policy for Virtual Volumes.

2. Assign the Virtual Volumes storage policy to the virtual machine.

   To guarantee that the Virtual Volumes datastore fulfills specific storage requirements when allocating a virtual machine, associate the Virtual Volumes storage policy with the virtual machine.

   See Assign Storage Policies to Virtual Machines.

3. Change default storage policy for a Virtual Volumes datastore.

   For virtual machines provisioned on Virtual Volumes datastores, VMware provides a default No Requirements policy. You cannot edit this policy, but you can designate a newly created policy as default.

   See Change the Default Storage Policy for a Datastore.

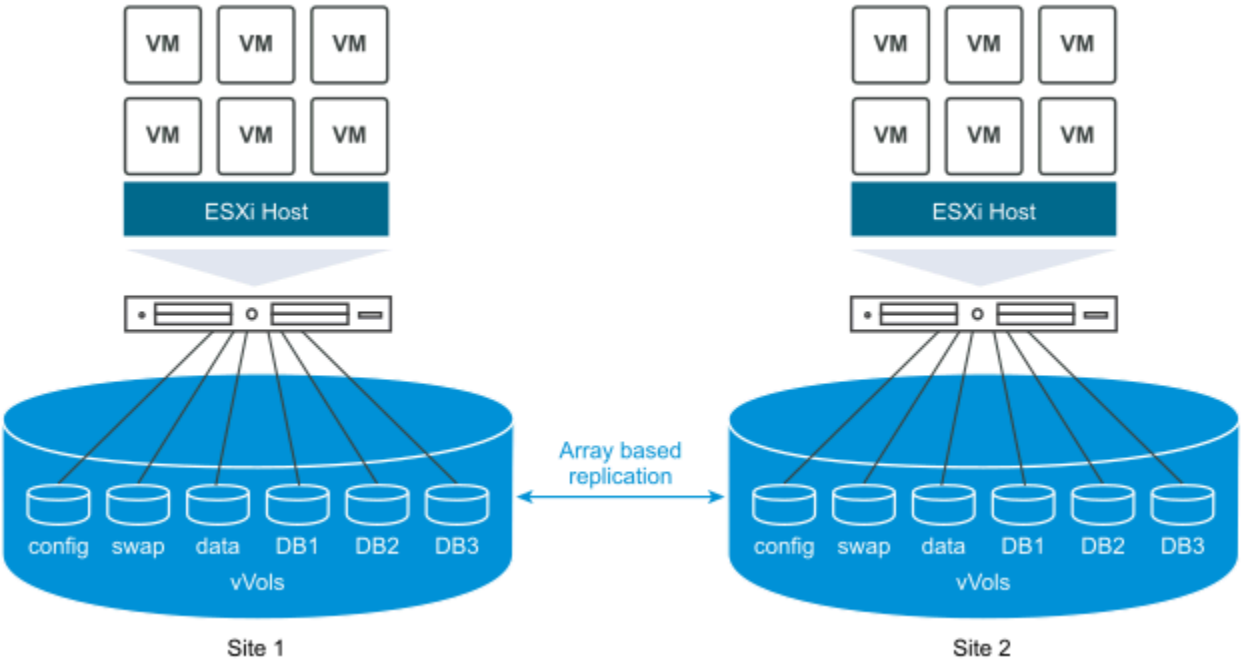
Virtual Volumes and Replication

Virtual Volumes supports replication and disaster recovery. With the array-based replication, you can off-load replication of virtual machines to your storage array and use full replication capabilities of the array. You can replicate a single VM object, such as a virtual disk. You can also group several VM objects or virtual machines to replicate them as a single unit.

Array-based replication is policy driven. After you configure your Virtual Volumes storage for replication, information about replication capabilities and replication groups is delivered from the array by the storage provider. This information shows in the VM Storage Policy interface of vCenter Server.

You use the VM storage policy to describe replication requirements for your virtual machines. The parameters that you specify in the storage policy depend on how your array implements replication. For example, your VM storage policy might include such parameters as the replication schedule, replication frequency, or recovery point objective (RPO). The policy might also indicate the replication target, a secondary site where your virtual machines are replicated, or specify whether replicas must be deleted.

By assigning the replication policy during VM provisioning, you request replication services for your virtual machine. After that, the array takes over the management of all replication schedules and processes.



Requirements for Replication with Virtual Volumes

When you enable Virtual Volumes with replication, in addition to general Virtual Volumes requirements, your environment must satisfy several specific prerequisites.

For general Virtual Volumes requirements, see Before You Enable Virtual Volumes.

Storage Requirements

Implementation of Virtual Volumes replication depends on your array and might be different for storage vendors. Generally, the following requirements apply to all vendors.

- The storage arrays that you use to implement replication must be compatible with Virtual Volumes.
- The arrays must integrate with the version of the storage (VASA) provider compatible with Virtual Volumes replication.
- The storage arrays must be replication capable and configured to use vendor-provided replication mechanisms. Typical configurations usually involve one or two replication targets. Any required configurations, such as pairing of the replicated site and the target site, must be also performed on the storage side.
- When applicable, replication groups and fault domains for Virtual Volumes must be preconfigured on the storage side.

For more information, contact your vendor and see *VMware Compatibility Guide*.

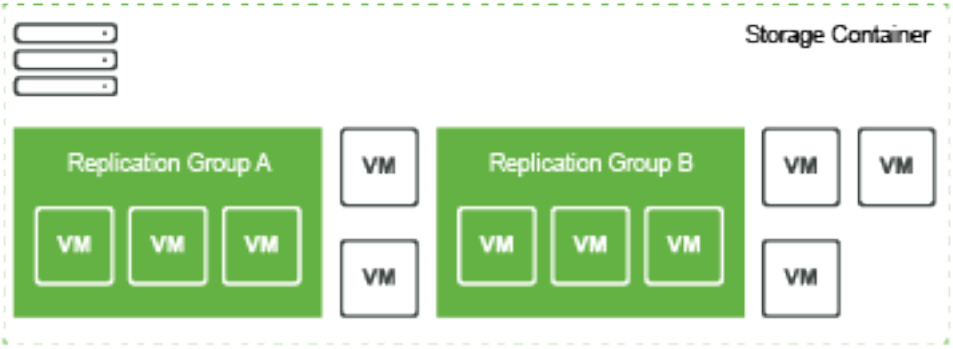
vSphere Requirements

- Use the vCenter Server and ESXi versions that support Virtual Volumes storage replication. vCenter Server and ESXi hosts that are older than 6.5 release do not support replicated Virtual Volumes storage. Any attempts to create a replicated VM on an incompatible host fail with an error. For information, see *VMware Compatibility Guide*.
- If you plan to migrate a virtual machine, make sure that target resources, such as the ESXi hosts and Virtual Volumes datastores, support storage replication.

Virtual Volumes and Replication Groups

When your storage offers replication services, in addition to storage containers and protocol endpoints, your storage administrator can configure replication groups on the storage side.

vCenter Server and ESXi can discover replication groups, but do not manage their life cycle. Replication groups, also called consistency groups, indicate which VMs and virtual disks must be replicated together to a target site. A single VM cannot span multiple replication groups.



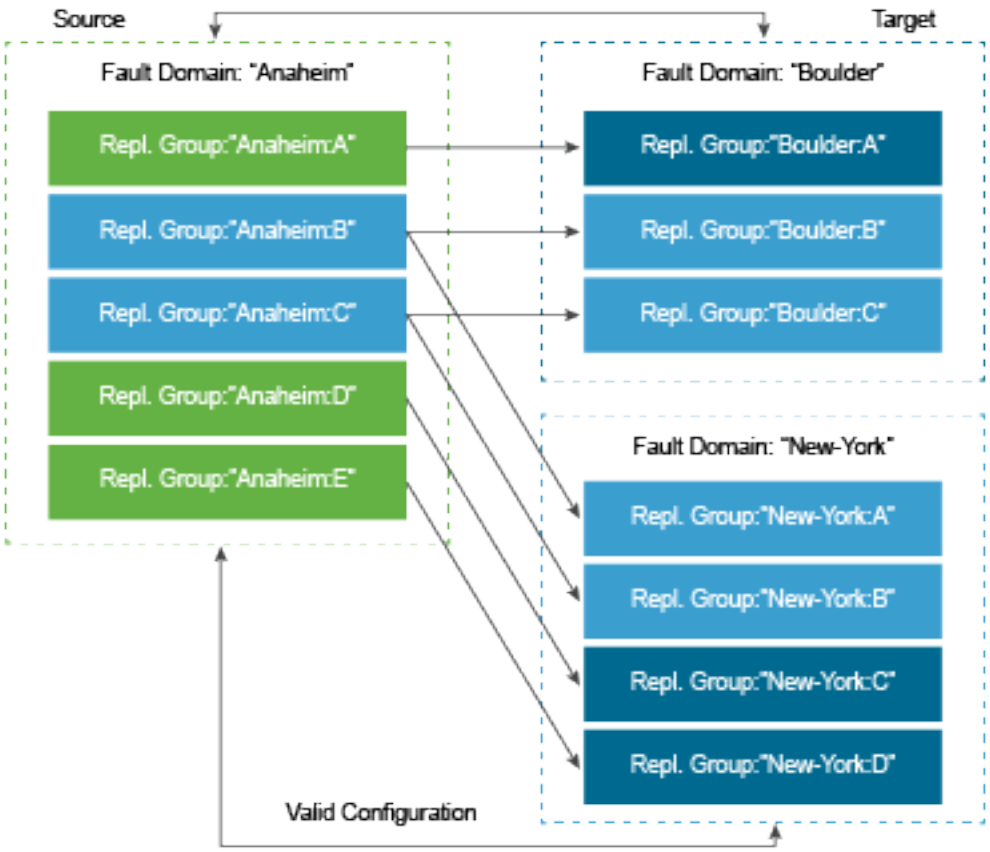
If no preconfigured groups are available, Virtual Volumes can use an automatic method. With the automatic method, Virtual Volumes creates a replication group on demand and associates this group with a Virtual Volumes object being provisioned. If you use the automatic replication group, all components of a virtual machine are assigned to the group. You cannot mix preconfigured and automatic replication groups for components of the same virtual machine.

Virtual Volumes and Fault Domains

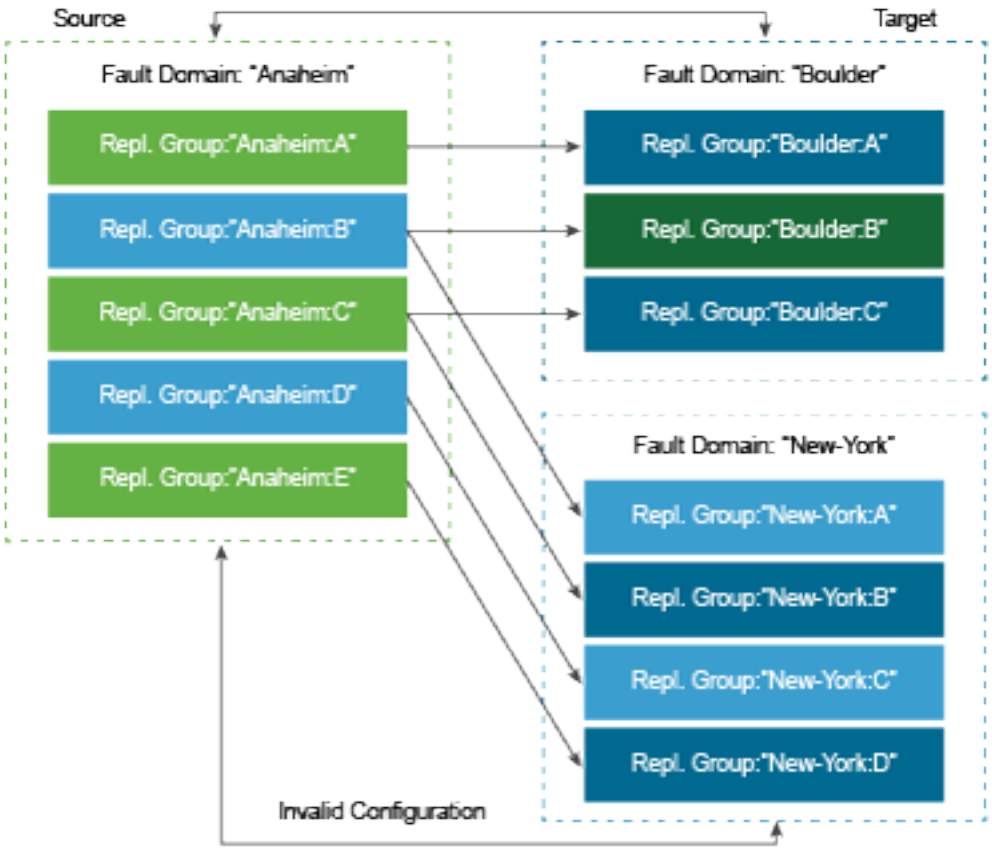
In the Virtual Volumes environment, fault domains define how specific replication groups must be combined when being replicated from a source to a target site.

Fault domains are configured and reported by the storage array, and are not exposed in the vSphere Client. The Storage Policy Based Management (SPBM) mechanism discovers fault domains and uses them for validation purposes during a virtual machine creation.

For example, provision two virtual machines, one associated with replication group Anaheim: B, the second associated with replication group Anaheim: C. SPBM validates the provisioning because each VM is in its own replication group with corresponding target fault domains.



Now provision two VMs, one associated with replication group Anaheim: B, the second associated with replication group Anaheim: D. This configuration is invalid. Both replication groups replicate to the New-York fault domain, however, only one replicates to the Boulder fault domain.



Virtual Volumes Replication Workflow

If information about replication capabilities of the Virtual Volumes storage array shows in vCenter Server, you can activate replication for your virtual machines.

The workflow to activate replication for your virtual machines includes steps typical for the virtual machine provisioning on Virtual Volumes storage.

1. Define the VM storage policy compatible with replication storage. The datastore-based rules of the policy must include the replication component. See Create a VM Storage Policy for Virtual Volumes.
   After you configure the storage policy that includes replication, vCenter Server discovers available replication groups.
2. Assign the replication policy to your virtual machine. If configured, select a compatible replication group, or use the automatic assignment. See Assign Storage Policies to Virtual Machines.

Replication Guidelines and Considerations

When you use replication with Virtual Volumes, specific considerations apply.

- You can apply the replication storage policy only to a configuration virtual volume and a data virtual volume. Other VM objects inherit the replication policy in the following way:
  - The memory virtual volume inherits the policy of the configuration virtual volume.
  - The digest virtual volume inherits the policy of the data virtual volume.
  - The swap virtual volume, which exists while a virtual machine is powered on, is excluded from replication.

- If you do not apply the replication policy to a VM disk, the disk is not replicated.
- The replication storage policy should not be used as a default storage policy for a datastore. Otherwise, the policy prevents you from selecting replication groups.
- Replication preserves snapshot history. If a snapshot was created and replicated, you can recover to the application consistent snapshot.
- You can replicate a linked clone. If a linked clone is replicated without its parent, it becomes a full clone.
- If a descriptor file belongs to a virtual disk of one VM, but resides in the VM home of another VM, both VMs must be in the same replication group. If the VMs are located in different replication groups, both of these replication groups must be failed over at the same time. Otherwise, the descriptor might become unavailable after the failover. As a result, the VM might fail to power on.
- In your Virtual Volumes with replication environment, you might periodically run a test failover workflow to ensure that the recovered workloads are functional after a failover.

  The resulting test VMs that are created during the test failover are fully functional and suitable for general administrative operations. However, certain considerations apply:
  - All VMs created during the test failover must be deleted before the test failover stops. The deletion ensures that any snapshots or snapshot-related virtual volumes that are part of the VM, such as the snapshot virtual volume, do not interfere with stopping of the test failover.
  - You can create full clones of the test VMs.
  - You can create fast clones only if the policy applied to the new VM contains the same replication group ID as the VM being cloned. Attempts to place the child VM outside of the replication group of the parent VM fail.

Best Practices for Working with Virtual Volumes

Observe the following recommendations when you use Virtual Volumes with ESXi and vCenter Server.

Guidelines and Limitations when Using Virtual Volumes

For the best experience with Virtual Volumes functionality, you must follow specific guidelines.

Virtual Volumes supports the following capabilities, features, and VMware products:

- With Virtual Volumes, you can use advanced storage services that include replication, encryption, deduplication, and compression on individual virtual disks. Contact your storage vendor for information about services they support with Virtual Volumes.
- Virtual Volumes functionality supports backup software that uses vSphere APIs - Data Protection. Virtual volumes are modeled on virtual disks. Backup products that use vSphere APIs - Data Protection are as fully supported on virtual volumes as they are on VMDK files on a LUN. Snapshots that the backup software creates using vSphere APIs - Data Protection look as non-vVols snapshots to vSphere and the backup software.

  Note: Virtual Volumes does not support SAN transport mode. vSphere APIs - Data Protection automatically selects an alternative data transfer method.

  For more information about integration with the vSphere Storage APIs - Data Protection, consult your backup software vendor.
- Virtual Volumes supports such vSphere features as vSphere vMotion, Storage vMotion, snapshots, linked clones, and DRS.
- You can use clustering products, such as Oracle Real Application Clusters, with Virtual Volumes. To use these products, you activate the multiwrite setting for a virtual disk stored on the Virtual Volumes datastore.

For more details, see the knowledge base article at http://kb.vmware.com/kb/2112039. For a list of features and products that Virtual Volumes functionality supports, see *VMware Product Interoperability Matrixes*.

Virtual Volumes Limitations

Improve your experience with Virtual Volumes by knowing the following limitations:

- Because the Virtual Volumes environment requires vCenter Server, you cannot use Virtual Volumes with a standalone host.
- Virtual Volumes functionality does not support RDMs.
- A Virtual Volumes storage container cannot span multiple physical arrays. Some vendors present multiple physical arrays as a single array. In such cases, you still technically use one logical array.
- Host profiles that contain Virtual Volumes datastores are vCenter Server specific. After you extract this type of host profile, you can attach it only to hosts and clusters managed by the same vCenter Server as the reference host.

Best Practices for Storage Container Provisioning

Follow these best practices when provisioning storage containers on the Virtual Volumes array side.

Creating Containers Based on Your Limits

Because storage containers apply logical limits when grouping virtual volumes, the container must match the boundaries that you want to apply.

Examples might include a container created for a tenant in a multitenant deployment, or a container for a department in an enterprise deployment.

- Organizations or departments, for example, Human Resources and Finance
- Groups or projects, for example, Team A and Red Team
- Customers

Putting All Storage Capabilities in a Single Container

Storage containers are individual datastores. A single storage container can export multiple storage capability profiles. As a result, virtual machines with diverse needs and different storage policy settings can be a part of the same storage container.

Changing storage profiles must be an array-side operation, not a storage migration to another container.

Avoiding Over-Provisioning Your Storage Containers

When you provision a storage container, the space limits that you apply as part of the container configuration are only logical limits. Do not provision the container larger than necessary for the anticipated use. If you later increase the size of the container, you do not need to reformat or repartition it.

Using Storage-Specific Management UI to Provision Protocol Endpoints

Every storage container needs protocol endpoints (PEs) that are accessible to ESXi hosts.

When you use block storage, the PE represents a proxy LUN defined by a T10-based LUN WWN. For NFS storage, the PE is a mount point, such as an IP address or DNS name, and a share name.

Typically, configuration of PEs is array-specific. When you configure PEs, you might need to associate them with specific storage processors, or with certain hosts. To avoid errors when creating PEs, do not configure them manually. Instead, when possible, use storage-specific management tools.

No Assignment of IDs Above Disk.MaxLUN to Protocol Endpoint LUNs

By default, an ESXi host can access LUN IDs that are within the range of 0 to 1023. If the ID of the protocol endpoint LUN that you configure is 1024 or greater, the host might ignore the PE.

If your environment uses LUN IDs that are greater than 1023, change the number of scanned LUNs through the `Disk.MaxLUN` parameter. See Change the Number of Scanned Storage Devices.

Best Practices for Virtual Volumes Performance

To ensure optimal Virtual Volumes performance results, follow these recommendations.

Using Different VM Storage Policies for Individual Virtual Volume Components

By default, all components of a virtual machine in the Virtual Volumes environment get a single VM storage policy. However, different components might have different performance characteristics, for example, a database virtual disk and a corresponding log virtual disk. Depending on performance requirements, you can assign different VM storage policies to individual virtual disks and to the VM home file, or config-vVol.

When you use the vSphere Client, you cannot change the VM storage policy assignment for swap-vVol, memory-vVol, or snapshot-vVol.

See Create a VM Storage Policy for Virtual Volumes.

Getting a Host Profile with Virtual Volumes

The best way to get a host profile with Virtual Volumes is to configure a reference host and extract its profile. If you manually edit an existing host profile in the vSphere Client and attach the edited profile to a new host, you might trigger compliance errors. Other unpredictable problems might occur. For more details, see the VMware Knowledge Base article 2146394.

Monitoring I/O Load on Individual Protocol Endpoint

- All virtual volume I/O goes through protocol endpoints (PEs). Arrays select protocol endpoints from several PEs that are accessible to an ESXi host. Arrays can do load balancing and change the binding path that connects the virtual volume and the PE. See Binding and Unbinding Virtual Volumes to Protocol Endpoints.
- On block storage, ESXi gives a large queue depth to I/O because of a potentially high number of virtual volumes. The `Scsi.ScsiVVolPESNRO` parameter controls the number of I/O that can be queued for PEs. You can configure the parameter on the Advanced System Settings page of the vSphere Client.

Monitoring Array Limitations

A single VM might occupy multiple virtual volumes. See Virtual Volume Objects.

Suppose that your VM has two virtual disks, and you take two snapshots with memory. Your VM might occupy up to 10 Virtual Volumes objects: a config-vVol, a swap-vVol, two data-vVols, four snapshot-vVols, and two memory snapshot-vVols.

Ensuring that Storage Provider Is Available

To access Virtual Volumes storage, your ESXi host requires a storage provider (VASA provider). To ensure that the storage provider is always available, follow these guidelines:

- Do not migrate a storage provider VM to Virtual Volumes storage.
- Back up your storage provider VM.
- When appropriate, use vSphere HA or Site Recovery Manager to protect the storage provider VM.

Troubleshooting Virtual Volumes

The troubleshooting topics provide solutions to problems that you might encounter when using Virtual Volumes.

Virtual Volumes and esxcli Commands

You can use the `esxcli storage vvol` commands to troubleshoot your Virtual Volumes environment.

The following command options are available.

Table 226: esxcli storage vvol commands

Namespace	Command Option	Description
`esxcli storage core device`	list	Identify protocol endpoints. The output entry `Is VVOL PE: true` indicates that the storage device is a protocol endpoint.
`esxcli storage vvol daemon`	unbindall	Unbind all virtual volumes from all VASA providers known to the ESXi host.
`esxcli storage vvol protocolendpoint`	list	List all protocol endpoints that your host can access.
`esxcli storage vvol storagecontainer`	list abandonedvvol scan	List all available storage containers. Scan the specified storage container for abandoned virtual volumes.
`esxcli storage vvol vasacontext`	get	Show the VASA context (VC UUID) associated with the host.
`esxcli storage vvol vasaprovider`	list	List all storage (VASA) providers associated with the host.

Collecting Statistical Information for Virtual Volumes

You can use the `vvol stats` command in your ESXi host to track performance statistics.

The following command options are available.

Command	Description	Options
`esxcli storage vvol stats get`	Get statistics for all VASA providers (default), or for specified namespace or entity in the given namespace.	`-e|--entity=`*`str`* Enter entity ID. `-n|--namespace=`*`str`* Enter node namespace expression. `-r|--raw` Enable raw format output.
`esxcli storage vvol stats list`	List all the statistics nodes (default), or nodes under a specified namespace.	`-n|--namespace=`*`str`* Enter node namespace expression.
`esxcli storage vvol stats enable`	Enable statistics tracking for the complete namespace.	
`esxcli storage vvol stats disable`	Disable statistics tracking for the complete namespace.	
`esxcli storage vvol stats add`	Enable statistics tracking for a specific entity under a specific namespace.	`-e|--entity=`*`str`* Enter entity ID. `-n|--namespace=`*`str`* Enter node namespace expression.
`esxcli storage vvol stats remove`	Removes specific entity for statistics tracking under the specified namespace.	`-e|--entity=`*`str`* Enter entity ID. `-n|--namespace=`*`str`* Enter node namespace expression.
`esxcli storage vvol stats reset`	Reset the statistics counter for the specified statistics namespace or entity.	`-e|--entity=`*`str`* Enter entity ID.

Command	Description	Options
		`-n|--namespace=str` Enter node namespace expression.

Virtual Volumes Datastore Is Inaccessible

After you create a Virtual Volumes datastore, it remains inaccessible.

The vSphere Client shows the datastore as inaccessible. You cannot use the datastore for virtual machine provisioning.

This problem might occur when you fail to configure protocol endpoints for the SCSI-based storage container that is mapped to the virtual datastore. Like traditional LUNs, SCSI protocol endpoints need to be configured so that an ESXi host can detect them.

Before creating virtual datastores for SCSI-based containers, make sure to configure protocol endpoints on the storage side.

Failures When Migrating VMs or Deploying VM OVFs to Virtual Volumes Datastores

Your attempts to migrate a virtual machine or to deploy a VM OVF to Virtual Volumes datastores fail.

An OVF template or a VM being migrated from a nonvirtual datastore might include additional large files, such as ISO disk images, DVD images, and image files. If these additional files cause the configuration virtual volume to exceed its 4-GB limit, migration or deployment to a virtual datastore fails.

The configuration virtual volume, or config-vVol, contains various VM-related files. On traditional nonvirtual datastores, these files are stored in the VM home directory. Similar to the VM home directory, the config-vVol typically includes the VM configuration file, virtual disk and snapshot descriptor files, log files, lock files, and so on.

On virtual datastores, all other large-sized files, such as virtual disks, memory snapshots, swap, and digest, are stored as separate virtual volumes.

Config-vVols are created as 4-GB virtual volumes. Generic content of the config-vVol usually consumes only a fraction of this 4-GB allocation, so config-vVols are typically thin-provisioned to conserve backing space. Any additional large files, such as ISO disk images, DVD images, and image files, might cause the config-vVol to exceed its 4-GB limit. If such files are included in an OVF template, deployment of the VM OVF to Virtual Volumes storage fails. If these files are part of an existing VM, migration of that VM from a traditional datastore to Virtual Volumes storage also fails.

Note: Starting with vSphere 7.0 Update 2, partners can increase the config-vVol to above 4 GB. Work with your Virtual Volumes partner on implementing this if it is supported by your partner and applicable to your environment.

- For VM migration. Before migrating a VM from a traditional datastore to a virtual datastore, remove excess content from the VM home directory to keep the config-vVol under the 4-GB limit.
- For OVF deployment. Because you cannot deploy an OVF template that contains excess files directly to a virtual datastore, first deploy the VM to a nonvirtual datastore. Remove any excess content from the VM home directory, and migrate the resulting VM to Virtual Volumes storage.

Filtering Virtual Machine I/O

I/O filters are software components that can be installed on ESXi hosts and can offer additional data services to virtual machines. The filters process I/O requests, which move between the guest operating system of a virtual machine and virtual disks.

The I/O filters can be offered by VMware or created by third parties through vSphere APIs for I/O Filtering (VAIO).

About I/O Filters

I/O filters can gain direct access to the virtual machine I/O path. You can enable the I/O filter for an individual virtual disk level. The I/O filters are independent of the storage topology.

VMware offers certain categories of I/O filters. In addition, third-party vendors can create the I/O filters. Typically, they are distributed as packages that provide an installer to deploy the filter components on vCenter Server and ESXi host clusters.

After the I/O filters are deployed, vCenter Server configures and registers an I/O filter storage provider, also called a VASA provider, for each host in the cluster. The storage providers communicate with vCenter Server and make data services offered by the I/O filter visible in the VM Storage Policies interface. You can reference these data services when defining common rules for a VM policy. After you associate virtual disks with this policy, the I/O filters are enabled on the virtual disks.

Datastore Support

I/O filters can support all datastore types including the following:

- VMFS
- NFS 3
- NFS 4.1
- vVol
- vSAN

Types of I/O Filters

VMware provides certain categories of I/O filters that are installed on your ESXi hosts. In addition, VMware partners can create the I/O filters through the vSphere APIs for I/O Filtering (VAIO) developer program. The I/O filters can serve multiple purposes.

The supported types of filters include the following:

- Replication. Replicates all write I/O operations to an external target location, such as another host or cluster.
- Encryption. Offered by VMware. Provides encryption mechanisms for virtual machines. For more information, see the *vSphere Security* documentation.
- Caching. Implements a cache for virtual disk data. The filter can use a local flash storage device to cache the data and increase the IOPS and hardware utilization rates for the virtual disk. If you use the caching filter, you might need to configure a Virtual Flash Resource.
- Storage I/O control. Offered by VMware. Throttles the I/O load towards a datastore and controls the amount of storage I/O that is allocated to virtual machines during periods of I/O congestion. For more information, see the *vSphere Resource Management* documentation.

Note: You can install several filters from the same category, such as caching, on your ESXi host. However, you can have only one filter from the same category per virtual disk.

I/O Filtering Components

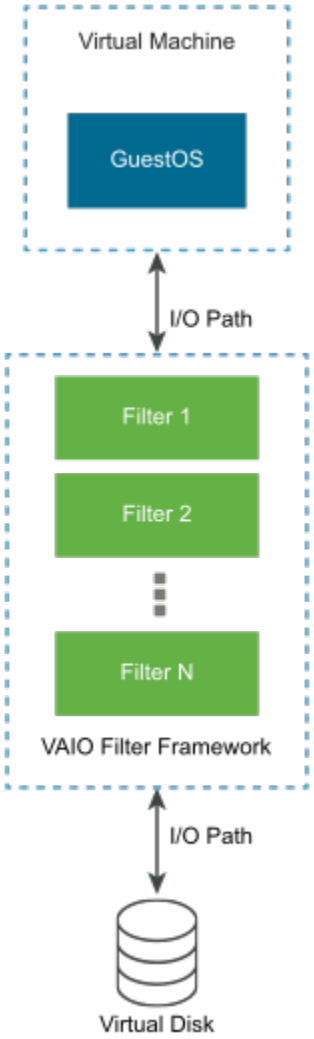
Several components are involved in the I/O filtering process.

The basic components of I/O filtering include the following:

VAIO Filter Framework	A combination of user world and VMkernel infrastructure provided by ESXi. With the framework, you can add filter plug-ins to the I/O path to and from virtual disks. The infrastructure includes an I/O filter storage provider (VASA provider). The provider integrates

	with the Storage Policy Based Management (SPBM) system and exports filter capabilities to vCenter Server.
I/O Filter Plug-In	A software component provided by VMware or developed by VMware partners that intercepts and filters I/O data in transit between virtual disks and guest operating systems. If VMware partners develop the I/O filter, the filter might include additional optional components that help in its configuration and management.

The following figure illustrates the components of I/O filtering and the flow of I/O between the guest OS and the virtual disk.



Each Virtual Machine Executable (VMX) component of a virtual machine contains a Filter Framework that manages the I/O filter plug-ins attached to the virtual disk. The Filter Framework invokes filters when the I/O requests move between the guest operating system and the virtual disk. Also, the filter intercepts any I/O access towards the virtual disk that happens outside of a running VM.

The filters run sequentially in a specific order. For example, a replication filter executes before a cache filter. More than one filter can operate on the virtual disk, but only one for each category.

Once all filters for the particular disk verify the I/O request, the request moves to its destination, either the VM or the virtual disk.

Because the filters run in user space, any filter failures impact only the VM, but do not affect the ESXi host.

Storage Providers for I/O Filters

When I/O filters are installed on ESXi hosts, the I/O filter framework configures and registers a storage provider, also called a VASA provider, for each host in the cluster.

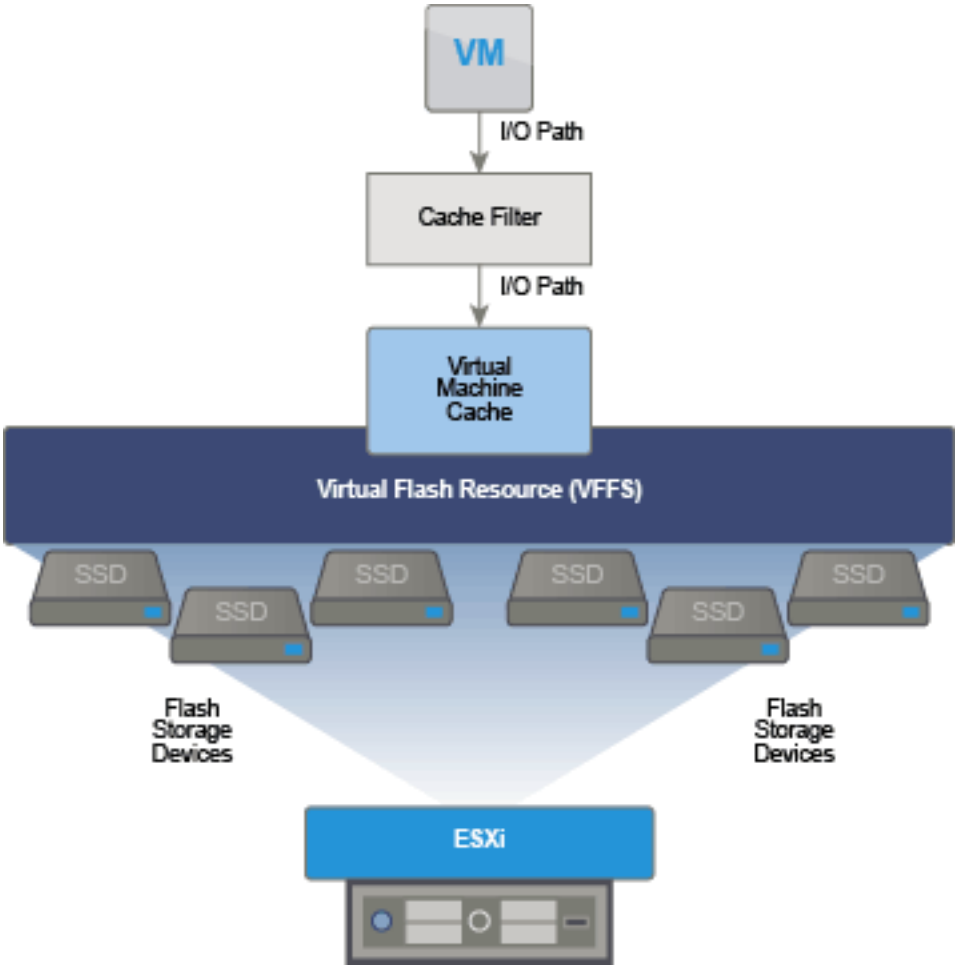
Storage providers for I/O filtering are software components that are offered by vSphere. They integrate with I/O filters and report data service capabilities that I/O filters support to vCenter Server.

The capabilities populate the VM Storage Policies interface and can be referenced in a VM storage policy. You then apply this policy to virtual disks, so that the I/O filters can process I/O for the disks.

Using Flash Storage Devices with Cache I/O Filters

A cache I/O filter can use a local flash device to cache virtual machine data.

If your caching I/O filter uses local flash devices, you need to configure a virtual flash resource, also known as VFFS volume. You configure the resource on your ESXi host before activating the filter. While processing the virtual machine read I/Os, the filter creates a virtual machine cache and places it on the VFFS volume.



To set up a virtual flash resource, you use flash devices that are connected to your host. To increase the capacity of your virtual flash resource, you can add more flash drives. An individual flash drive must be exclusively allocated to a virtual

flash resource and cannot be shared with any other vSphere service, such as vSAN or VMFS. See Set Up Virtual Flash Resource.

System Requirements for I/O Filters

To be able to use I/O filters in your environment, you must follow specific requirements.

The following requirements apply.

- Use the latest version of ESXi and vCenter Server compatible with I/O filters. Older versions might not support I/O filters, or provide only partial support.
- Check for any additional requirements that individual partner solutions might have. In specific cases, your environment might need flash devices, extra physical memory, or network connectivity and bandwidth. For information, contact your vendor or your VMware representative.
- Web server to host partner packages for filter installation. The server must remain available after initial installation. When a new host joins the cluster, the server pushes appropriate I/O filter components to the host.

Configure I/O Filters in the vSphere Environment

To set up data services that the I/O filters provide for your virtual machines, follow several steps.

- Create a cluster that includes at least one ESXi host.
- For information about I/O filters provided by third parties, contact your vendor or your VMware representative.

Install I/O Filters in a Cluster

If you use I/O filters provided by third parties, install the I/O filters in an ESXi host cluster.

- Required privileges: **Host.Configuration.Query patch**.
- Verify that the I/O filter solution is certified by VMware.

VMware partners create I/O filters through the vSphere APIs for I/O Filtering (VAIO) developer program.

The filter packages are distributed as solution bundle ZIP packages that can include I/O filter daemons, I/O filter libraries, CIM providers, and other associated components.

Typically, to deploy the filters, you run installers provided by vendors. Installation is performed at an ESXi cluster lever. You cannot install the filters on selected hosts directly.

Note: If you plan to install I/O filters on the vSphere 7.0 and later cluster, your cluster cannot include ESXi 6.x hosts. Filters built using the vSphere 6.x VAIO program cannot work on ESXi 7.0 and later hosts because the CIM provider is 32-bit on ESXi 6.x and 64-bit on ESXi 7.0 and later. In turn, filters built using the vSphere 7.0 and later VAIO program are not supported on ESXi 6.x hosts.

Run the installer that the vendor provided.

The installer deploys the appropriate I/O filter extension on vCenter Server and the filter components on all hosts within a cluster.

A storage provider, also called a VASA provider, is automatically registered for every ESXi host in the cluster. Successful auto-registration of the I/O filter storage providers triggers an event at the host level. If the storage providers fail to auto-register, the system raises alarms on the hosts.

View I/O Filters and Storage Providers

Use the vSphere Client to review I/O filters available in your environment and verify that the I/O filter providers appear as expected and are active.

When you install a third-party I/O filter, a storage provider, also called VASA provider, is automatically registered for every ESXi host in the cluster. Successful auto-registration of the I/O filter storage providers triggers an event at the host level. If the storage providers fail to auto-register, the system raises alarms on the hosts.

1. Verify that the I/O filter storage providers appear as expected and are active.
   a) Navigate to vCenter Server.
   b) Click the **Configure** tab, and click **Storage Providers**.
   c) Review the storage providers for I/O filters.

   When the I/O filter providers are properly registered, capabilities and data services that the filters offer populate the VM Storage Policies interface.
2. Verify that the I/O filter components are listed on your cluster and ESXi hosts.

Option	Actions
View I/O filters on a cluster	1. Navigate to the cluster. 2. Click the **Configure** tab. 3. Under **Configuration**, click **I/O Filters** to review the filters installed in the cluster.
View I/O filters on a host	1. Navigate to the host. 2. Click the **Configure** tab. 3. Under **Storage**, click **I/O Filters** to review the filters installed on the host.

Enable I/O Filter Data Services on Virtual Disks

Enabling data services that I/O filters provide is a two-step process. You create a virtual machine policy based on data services that the I/O filters provide, and then attach this policy to a virtual machine.

For the caching I/O filters, configure the virtual flash resource on your ESXi host before activating the filter. See Set Up Virtual Flash Resource.

1. Define a VM policy based on I/O filter services.

   Make sure that the virtual machine policy lists data services provided by the I/O filters.

   See Create a VM Storage Policy for Host-Based Data Services.
2. Assign the I/O filter policy to a virtual machine.

   To activate data services that the I/O filter provides, associate the I/O filter policy with virtual disks. You can assign the policy when you provision the virtual machine.

   See Assign the I/O Filter Policy to Virtual Machines.

If you later want to disable the I/O filter for a virtual machine, you can remove the filter rules from the VM storage policy and re-apply the policy. See Edit or Clone a VM Storage Policy. Or you can edit the settings of the virtual machine and select a different storage policy that does not include the filter.

Assign the I/O Filter Policy to Virtual Machines

To activate data services that I/O filters provide, associate the I/O filter policy with virtual disks. You can assign the policy when you create or edit a virtual machine.

Verify that the I/O filter is installed on the ESXi host where the virtual machine runs.

You can assign the I/O filter policy during an initial deployment of a virtual machine. This topic describes how to assign the policy when you create a new virtual machine. For information about other deployment methods, see the *vSphere Virtual Machine Administration* documentation.

Note: You cannot change or assign the I/O filter policy when migrating or cloning a virtual machine.

1. Start the virtual machine provisioning process and follow the appropriate steps.
2. Assign the same storage policy to all virtual machine files and disks.
   a) On the **Select storage** page, select a storage policy from the **VM Storage Policy** drop-down menu.
   b) Select the datastore from the list of compatible datastores and click **Next**.

      The datastore becomes the destination storage resource for the virtual machine configuration file and all virtual disks. The policy also activates I/O filter services for the virtual disks.
3. Change the VM storage policy for the virtual disk.

   Use this option to enable I/O filters just for your virtual disks.
   a) On the **Customize hardware** page, expand the **New hard disk** pane.
   b) From the **VM storage policy** drop-down menu, select the storage policy to assign to the virtual disk.
   c) Optional: Change the storage location of the virtual disk.

      Use this option to store the virtual disk on a datastore other than the datastore where the VM configuration file resides.
4. Complete the virtual machine provisioning process.

After you create the virtual machine, the **Summary** tab displays the assigned storage policies and their compliance status. You can later change the virtual policy assignment. See Change Storage Policy Assignment for Virtual Machine Files and Disks.

Managing I/O Filters

You can run the installer provided by your vendor to install, uninstall, or upgrade I/O filters.

When you work with I/O filters, the following considerations apply:

- vCenter Server uses ESX Agent Manager (EAM) to install and uninstall I/O filters. As an administrator, never invoke EAM APIs directly for EAM agencies that are created or used by vCenter Server. All operations related to I/O filters must go through VIM APIs. If you accidentally modify an EAM agency that was created by vCenter Server, you must revert the changes. If you accidentally destroy an EAM agency that is used by I/O filters, you must call `Vim.IoFilterManager#uninstallIoFilter` to uninstall the affected I/O filters. After uninstalling, perform a fresh reinstall.
- When a new host joins the cluster that has I/O filters, the filters installed on the cluster are deployed on the host. vCenter Server registers the I/O filter storage provider for the host. Any cluster changes become visible in the VM Storage Policies interface of the vSphere Client.
- When you move a host out of a cluster or remove it from vCenter Server, the I/O filters are uninstalled from the host. vCenter Server unregisters the I/O filter storage provider.
- If you use a stateless ESXi host, it might lose its I/O filter VIBs during a reboot. vCenter Server checks the bundles installed on the host after it reboots, and pushes the I/O filter VIBs to the host if necessary.

Uninstall I/O Filters from a Cluster

You can uninstall I/O filters deployed in an ESXi host cluster.

- Required privileges: **Host.Config.Patch**.

1. Uninstall the I/O filter by running the installer that your vendor provides.

   During uninstallation, a third party I/O filter installer automatically places the hosts into maintenance mode.

   If the uninstallation is successful, the filter and any related components are removed from the hosts.

2. Verify that the I/O filter components are properly uninstalled from your ESXi hosts. Use one of the following methods:

   - Run the `esxcli software vib list` command.
   - View the I/O filters in the vSphere Client. See View I/O Filters and Storage Providers.

   The uninstalled filter no longer appears on the list.

Upgrade I/O Filters in a Cluster

After you upgrade your ESXi hosts to version 7.0 and later, use installers provided by I/O filter vendors to upgrade I/O filters deployed in the ESXi host cluster.

- Required privileges: **Host.Config.Patch**.
- Upgrade your hosts to ESXi 7.0 and later. If you use vSphere Lifecycle Manager for the upgrade, see the *Managing Host and Cluster Lifecycle* documentation.

When you upgrade an ESXi 6.x host that has custom I/O filter VIBs to version 7.0 and later, all supported custom VIBs are migrated. However, the legacy I/O filters cannot work on ESXi 7.0 and later. The filters generally include 32 bit CIM providers, while ESXi 7.0 and later requires 64 bit CIM applications. You need to upgrade the legacy filters to make them compatible.

An upgrade consists of uninstalling the old filter components and replacing them with the new filter components. To determine whether an installation is an upgrade, vCenter Server checks the names and versions of existing filters. If the existing filter names match the names of the new filters but have different versions, the installation is considered an upgrade.

1. To upgrade the filter, run the vendor-provided installer.

   During the upgrade, a third party I/O filter installer automatically places the hosts into maintenance mode.

   The installer identifies any existing filter components and removes them before installing the new filter components.

2. Verify that the I/O filter components are properly upgraded in your ESXi hosts. Use one of the following methods:

   - Run the `esxcli software vib list` command.
   - View the I/O filters in the vSphere Client. See View I/O Filters and Storage Providers.

After the upgrade, the system places the hosts back into operational mode.

I/O Filter Guidelines and Best Practices

When you use I/O filters in your environment, follow specific guidelines and best practices.

- Because I/O filters are datastore-agnostic, all types of datastores, including VMFS, NFS, Virtual Volumes, and vSAN, are compatible with I/O filters.
- I/O filters support RDMs in virtual compatibility mode. No support is provided to RDMs in physical compatibility mode.
- You cannot change or assign the I/O filter policy while migrating or cloning a virtual machine. You can change the policy after you complete the migration or cloning.
- When you clone or migrate a virtual machine with I/O filter policy from one host to another, make sure that the destination host has a compatible filter installed. This requirement applies to migrations initiated by an administrator or by such functionalities as HA or DRS.
- When you convert a template to a virtual machine, and the template is configured with I/O filter policy, the destination host must have the compatible I/O filter installed.

- If you use vCenter Site Recovery Manager to replicate virtual disks, the resulting disks on the recovery site do not have the I/O filter policies. You must create the I/O filter policies in the recovery site and reattach them to the replicated disks.
- If your virtual machine has a snapshot tree associated with it, you cannot add, change, or remove the I/O filter policy for the virtual machine.

Migrating Virtual Machines with I/O Filters

When you migrate a virtual machine with I/O filters, specific considerations apply.

If you use Storage vMotion to migrate a virtual machine with I/O filters, a destination datastore must be connected to hosts with compatible I/O filters installed.

You might need to migrate a virtual machine with I/O filters across different types of datastores, for example between VMFS and Virtual Volumes. If you do so, make sure that the VM storage policy includes rule sets for every type of datastore you are planning to use. For example, if you migrate your virtual machine between the VMFS and Virtual Volumes datastores, create a mixed VM storage policy that includes the following rules:

- Common Rules for the I/O filters
- Rule Set 1 for the VMFS datastore. Because Storage Policy Based Management does not offer an explicit VMFS policy, the rule set must include tag-based rules for the VMFS datastore.
- Rule Set 2 for the Virtual Volumes datastore

When Storage vMotion migrates the virtual machine, the correct rule set that corresponds to the target datastore is selected. The I/O filter rules remain unchanged.

If you do not specify rules for datastores and define only Common Rules for the I/O filters, the system applies default storage policies for the datastores.

Handling I/O Filter Installation Failures

Typically, all ESXi hosts in a cluster have the same set of I/O filters installed. Occasionally, failures might happen during installation.

If an I/O filter installation fails on a host, the system generates events that report the failure. In addition, an alarm on the host shows the reason for the failure. Examples of failures include the following:

- The VIB URL is not accessible from the host.
- The VIB has an invalid format.
- The VIB requires the host to be in maintenance mode for an upgrade or uninstallation.
- The VIB requires the host to reboot after the installation or uninstallation.
- Attempts to put the host in maintenance mode fail because the virtual machine cannot be evacuated from the host.
- The VIB requires manual installation or uninstallation.

vCenter Server can resolve some failures. You might have to intervene for other failures. For example, you might need to edit the VIB URL, manually evacuate or power off virtual machines, or manually install or uninstall VIBs.

Install I/O Filters on a Single ESXi Host

For troubleshooting purposes, you can download an ESXi component of the I/O filter, packaged as a VIB file, and install it on the ESXi host. Use the `esxcli` command to install the VIB file.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. Install the VIBs by running the following command:

   ```
   esxcli software vib install --depot path_to_VMware_vib_ZIP_file
   ```

Options for the `install` command allow you to perform a dry run, specify a specific VIB, bypass acceptance-level verification, and so on. Do not bypass verification on production systems. See the *ESXCLI Reference* documentation.

2. Verify that the VIBs are installed on your ESXi host.

   ```
   esxcli software vib list
   ```

Storage Hardware Acceleration

The hardware acceleration functionality enables the ESXi host to integrate with compliant storage systems. The host can offload certain virtual machine and storage management operations to the storage systems. With the storage hardware assistance, your host performs these operations faster and consumes less CPU, memory, and storage fabric bandwidth.

Block storage devices, Fibre Channel and iSCSI, and NAS devices support the hardware acceleration.

Hardware Acceleration Benefits

When the hardware acceleration functionality is supported, the host can get hardware assistance and perform several tasks faster and more efficiently.

The host can get assistance with the following activities:

- Migrating virtual machines with Storage vMotion
- Deploying virtual machines from templates
- Cloning virtual machines or templates
- VMFS clustered locking and metadata operations for virtual machine files
- Provisioning thick virtual disks
- Creating fault-tolerant virtual machines
- Creating and cloning thick disks on NFS datastores

Hardware Acceleration Requirements

The hardware acceleration functionality works only if you use an appropriate host and storage array combination.

Table 227: Hardware Acceleration Storage Requirements

ESXi	Block Storage Devices	NAS Devices
ESXi	Support T10 SCSI standard, or block storage plug-ins for array integration (VAAI)	Support NAS plug-ins for array integration

Note: If your SAN or NAS storage fabric uses an intermediate appliance in front of a storage system that supports hardware acceleration, the intermediate appliance must also support hardware acceleration and be properly certified. The intermediate appliance might be a storage virtualization appliance, I/O acceleration appliance, encryption appliance, and so on.

Hardware Acceleration Support Status

For each storage device and datastore, the vSphere Client display the hardware acceleration support status.

The status values are Unknown, Supported, and Not Supported. The initial value is Unknown.

For block devices, the status changes to Supported after the host successfully performs the offload operation. If the offload operation fails, the status changes to Not Supported. The status remains Unknown if the device provides partial hardware acceleration support.

With NAS, the status becomes Supported when the storage can perform at least one hardware offload operation.

When storage devices do not support or provide partial support for the host operations, your host reverts to its native methods to perform unsupported operations.

Hardware Acceleration for Block Storage Devices

With hardware acceleration, your host can integrate with block storage devices, Fibre Channel or iSCSI, and use certain storage array operations.

ESXi hardware acceleration supports the following array operations:

- Full copy, also called clone blocks or copy offload. Enables the storage arrays to make full copies of data within the array without having the host read and write the data. This operation reduces the time and network load when cloning virtual machines, provisioning from a template, or migrating with vMotion.
- Block zeroing, also called write same. Enables storage arrays to zero out a large number of blocks to provide newly allocated storage, free of previously written data. This operation reduces the time and network load when creating virtual machines and formatting virtual disks.
- Hardware assisted locking, also called atomic test and set (ATS). Supports discrete virtual machine locking without use of SCSI reservations. This operation allows disk locking per sector, instead of the entire LUN as with SCSI reservations.

Check with your vendor for the hardware acceleration support. Certain storage arrays require that you activate the support on the storage side.

On your host, the hardware acceleration is enabled by default. If your storage does not support the hardware acceleration, you can disable it.

In addition to hardware acceleration support, ESXi includes support for array thin provisioning. For information, see ESXi and Array Thin Provisioning.

Disable Hardware Acceleration for Block Storage Devices

On your host, the hardware acceleration for block storage devices is enabled by default. You can use the vSphere Client advanced settings to disable the hardware acceleration operations.

As with any advanced settings, before you disable the hardware acceleration, consult with the VMware support team.

1. In the vSphere Client, navigate to the ESXi host.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. Change the value for any of the options to 0 (disabled):
   - VMFS3.HardwareAcceleratedLocking
   - DataMover.HardwareAcceleratedMove
   - DataMover.HardwareAcceleratedInit

Managing Hardware Acceleration on Block Storage Devices

To integrate with the block storage arrays, vSphere uses the ESXi extensions called Storage APIs - Array Integration (VAAI). With this integration, vSphere can use the array hardware operations.

In the vSphere 5.x and later releases, these extensions are implemented as the T10 SCSI commands. As a result, with the devices that support the T10 SCSI standard, your ESXi host can communicate directly and does not require the VAAI plug-ins.

If the device does not support T10 SCSI or provides partial support, ESXi reverts to using the VAAI plug-ins, installed on your host. The host can also use a combination of the T10 SCSI commands and plug-ins. The VAAI plug-ins are vendor-

specific and can be either VMware or partner developed. To manage the VAAI capable device, your host attaches the VAAI filter and vendor-specific VAAI plug-in to the device.

For information about whether your storage requires VAAI plug-ins or supports hardware acceleration through T10 SCSI commands, see the *VMware Compatibility Guide* or contact your storage vendor.

You can use several `esxcli` commands to query storage devices for the hardware acceleration support information. For the devices that require the VAAI plug-ins, the claim rule commands are also available. For information about `esxcli` commands, see *Getting Started with ESXCLI*.

Display Hardware Acceleration Plug-Ins and Filter

To communicate with the devices that do not support the T10 SCSI standard, your host uses a single VAAI filter and a vendor-specific VAAI plug-in. Use the `esxcli` command to view the hardware acceleration filter and plug-ins currently loaded into your system.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Run the `esxcli storage core plugin list --plugin-class=`*`value`* command.

For *`value`*, enter one of the following parameters:

- Type `VAAI` to display plug-ins.

  The output of this command is similar to the following example:

  ```
  #esxcli storage core plugin list --plugin-class=VAAI
  Plugin name         Plugin class
  VMW_VAAIP_EQL       VAAI
  VMW_VAAIP_NETAPP    VAAI
  VMW_VAAIP_CX        VAAI
  ```

- Type `Filter` to display the Filter.

  The output of this command is similar to the following example:

  ```
  esxcli storage core plugin list --plugin-class=Filter
  Plugin name  Plugin class
  VAAI_FILTER  Filter
  ```

Verify Hardware Acceleration Support Status

Use the `esxcli` command to verify the hardware acceleration support status of a particular storage device.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Run the `esxcli storage core device list -d=`*`device_ID`* command.

The output shows the hardware acceleration, or VAAI, status that can be unknown, supported, or unsupported.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
 Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c)
 Size: 20480
 Device Type: Direct-Access
 Multipath Plugin: NMP
 XXXXXXXXXXXXXXX
 Attached Filters: VAAI_FILTER
 VAAI Status: supported
 XXXXXXXXXXXXXXX
```

Verify Hardware Acceleration Support Details

Use the `esxcli` command to query whether the block storage device provides the hardware acceleration support.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Run the `esxcli storage core device vaai status get -d=`*`device_ID`* command.

If a VAAI plug-in manages the device, the output shows the name of the plug-in attached to the device. The output also shows the support status for each T10 SCSI based primitive, if available. Output appears in the following example:

```
# esxcli storage core device vaai status get -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 VAAI Plugin Name: VMW_VAAIP_SYMM
 ATS Status: supported
 Clone Status: supported
 Zero Status: supported
 Delete Status: unsupported
```

List Hardware Acceleration Claim Rules

Each block storage device managed by a VAAI plug-in needs two claim rules. One claim rule specifies the hardware acceleration filter and another specifies the hardware acceleration plug-in for the device. You can use the `esxcli` commands to list the hardware acceleration filter and plug-in claim rules.

1. To list the filter claim rules, run the `esxcli storage core claimrule list --claimrule-class=Filter` command.

   In this example, the filter claim rules specify devices that the VAAI_FILTER filter claims.

   ```
   # esxcli storage core claimrule list --claimrule-class=Filter
   Rule Class   Rule   Class   Type   Plugin      Matches                   XCOPY Use Array Reported Values
    XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
   Filter       65430  runtime vendor VAAI_FILTER vendor=EMC model=SYMMETRIX                          False
                          False                              0
   Filter       65430  file    vendor VAAI_FILTER vendor=EMC model=SYMMETRIX                          False
                          False                              0
   Filter       65431  runtime vendor VAAI_FILTER vendor=DGC model=*                                  False
                          False                              0
   Filter       65431  file    vendor VAAI_FILTER vendor=DGC model=*                                  False
                          False                              0
   ```

2. To list the VAAI plug-in claim rules, run the `esxcli storage core claimrule list --claimrule-class=VAAI` command.

   In this example, the VAAI claim rules specify devices that the VAAI plug-in claims.

   ```
   esxcli storage core claimrule list --claimrule-class=VAAI
   Rule Class   Rule   Class   Type    Plugin         Matches                   XCOPY Use Array Reported Val-
   ues  XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
   VAAI         65430  runtime vendor  VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX
    False                          False                            0
   VAAI         65430  file    vendor  VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX
    False                          False                            0
   VAAI         65431  runtime vendor  VMW_VAAIP_CX   vendor=DGC model=*
    False                          False                            0
   VAAI         65431  file    vendor  VMW_VAAIP_CX   vendor=DGC model=*
    False                          False                            0
   ```

Add Hardware Acceleration Claim Rules

To configure the hardware acceleration for a new array, add two claim rules, one for the VAAI filter and another for the VAAI plug-in. For the new claim rules to be active, you first define the rules and then load them into your system.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. Define a new claim rule for the VAAI filter by running the `esxcli storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER` command.
2. Define a new claim rule for the VAAI plug-in by running the `esxcli storage core claimrule add --claimrule-class=VAAI` command.
3. Load both claim rules by running the following commands:

   ```
   esxcli storage core claimrule load --claimrule-class=Filter
   ```

   ```
   esxcli storage core claimrule load --claimrule-class=VAAI
   ```
4. Run the VAAI filter claim rule by using the `esxcli storage core claimrule run --claimrule-class=Filter` command.

   Note: Only the filter-class rules must be run. When the VAAI filter claims a device, it automatically finds the proper VAAI plug-in to attach.

   Defining Hardware Acceleration Claim Rules

   This example shows how to configure the hardware acceleration for IBM arrays using the VMW_VAAIP_T10 plug-in. Use the following sequence of commands. For information about the options that the command takes, see Add Multipathing Claim Rules.

   ```
   # esxcli storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER
   --type=vendor --vendor=IBM --autoassign
   ```

   ```
   # esxcli storage core claimrule add --claimrule-class=VAAI --plugin=VMW_VAAIP_T10
   --type=vendor --vendor=IBM --autoassign
   ```

   ```
   # esxcli storage core claimrule load --claimrule-class=Filter
   ```

   ```
   # esxcli storage core claimrule load --claimrule-class=VAAI
   ```

   ```
   # esxcli storage core claimrule run --claimrule-class=Filter
   ```

Configure XCOPY Parameters

XCOPY is one of the VAAI primitives that is used for offloading tasks to the storage array. For example, you can use XCOPY to offload such operations as migration or cloning of virtual machines to the array instead of consuming vSphere resources to perform these tasks.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

You can use the XCOPY mechanism with all storage arrays that support the SCSI T10 based VMW_VAAIP_T10 plug-in developed by VMware. To enable the XCOPY mechanism, create a claim rule of the VAAI class.

Use the following command and enter the XCOPY options:

```
esxcli storage core claimrule add --claimrule-class=VAAI
```

For information about the options that the command takes, see Add Multipathing Claim Rules.

Option	Description
-a|--xcopy-use-array-values	Use array reported values for XCOPY commands.

Option	Description
-s|--xcopy-use-multi-segs	Use multiple segments for XCOPY commands. Valid only when `--xcopy-use-array-values` is specified.
-m|--xcopy-max-transfer-size	Maximum transfer size in MB for the XCOPY commands when you use a transfer size different than array reported. Valid only when `--xcopy-use-array-values` is specified.
-k|--xcopy-max-transfer-size-kib	Maximum transfer size in KiB for the XCOPY commands when you use a transfer size different than array reported. Valid only if `--xcopy-use-array-values` is specified.

Configuring XCOPY

- `# esxcli storage core claimrule add -r 914 -t vendor -V XtremIO -M XtremApp -P VMW_VAAIP_T10 -c VAAI -a -s -k 64`
- `# esxcli storage core claimrule add -r 65430 -t vendor -V EMC -M SYMMETRIX -P VMW_VAAIP_SYMM -c VAAI -a -s -m 200`

Delete Hardware Acceleration Claim Rules

Use the `esxcli` command to delete existing hardware acceleration claim rules.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Run the following commands:

```
esxcli storage core claimrule remove -r claimrule_ID --claimrule-class=Filter
esxcli storage core claimrule remove -r claimrule_ID --claimrule-class=VAAI
```

Hardware Acceleration on NAS Devices

With the hardware acceleration, ESXi hosts can integrate with NAS devices and use several hardware operations that NAS storage provides. The hardware acceleration uses vSphere APIs for Array Integration (VAAI) to facilitate communications between the hosts and storage devices.

The VAAI NAS framework supports both versions of NFS storage, NFS 3 and NFS 4.1.

The VAAI NAS uses a set of storage primitives to offload storage operations from the host to the array. The following list shows the supported NAS operations:

Full File Clone

Supports an ability of NAS device to clone virtual disk files. This operation is similar to the VMFS block cloning, except that NAS devices clone entire files instead of file segments. Tasks that benefit from the full file clone operation include VM cloning, Storage vMotion, and deployment of VMs from templates.

When the ESXi host copies data with VAAI NAS, it does not need to read the data from the NAS and write back the data to the NAS. The host simply sends the copy command offloading it to the NAS. The copy process is done in the NAS, which reduces the load on the host.

Fast File Clone

This operation, also called array-based or native snapshots, offloads creation of virtual machine snapshots and linked clones to the array.

Reserve Space

Supports an ability of storage arrays to allocate space for a virtual disk file in the thick format.

Typically, when you create a virtual disk on an NFS datastore, the NAS server determines the allocation policy. The default allocation

	policy on most NAS servers is thin and does not guarantee backing storage to the file. However, the reserve space operation can instruct the NAS device to use vendor-specific mechanisms to reserve space for a virtual disk. As a result, you can create thick virtual disks on the NFS datastore if the backing NAS server supports the reserve space operation.
Extended Statistics	Supports visibility to space use on NAS devices. The operation enables you to query space utilization details for virtual disks on NFS datastores. The details include the size of a virtual disk and the space consumption of the virtual disk. This functionality is useful for thin provisioning.

With NAS storage devices, the hardware acceleration integration is implemented through vendor-specific NAS plug-ins. These plug-ins are typically created by vendors and are distributed as vendor packages. No claim rules are required for the NAS plug-ins to function.

Several tools for installing and updating NAS plug-ins are available. They include the `esxcli` commands and vSphere Lifecycle Manager. For more information, see the *VMware ESXi Upgrade* and *Managing Host and Cluster Lifecycle* documentation. For installation and update recommendations, see the Knowledge Base article.

Note: NAS storage vendors might provide additional settings that can affect the performance and operation of VAAI. Follow the vendor's recommendations and configure the appropriate settings on both the NAS storage array and ESXi. See your storage vendor documentation for more information.

Enable NAS Native Snapshots on Virtual Machines

If your deployment includes NAS arrays that support the vSphere APIs for Array Integration (VAAI), you can use the fast file clone technology, also called native NFS snapshots, to make virtual machine snapshots. With this technology, the NFS device copies the virtual machine without having the ESXi host read and write the data. This operation might reduce the time and network load when VM snapshots are created.

- Verify that the NAS array supports the fast file clone operation with the VAAI NAS program.
- On your ESXi host, install vendor-specific NAS plug-in that supports the fast file cloning with VAAI.
- Follow the recommendations of your NAS storage vendor to configure any required settings on both the NAS array and ESXi. See your storage vendor documentation for more information.

By default, all newly created VMs support traditional ESXi snapshot technology. To use the NFS native snapshot technology, enable it for the VM.

1. In the vSphere Client, right-click the virtual machine and select **Edit Settings**.
2. Click the **VM Options** tab and expand the **Advanced** menu.
3. Click **Edit Configuration** next to Configuration Parameters.
4. Configure the `snapshot.alwaysAllowNative` parameter.

   If the parameter exists, make sure that its value is set to True. If the parameter is not present, add it and set its value to True.

Name	Value
`snapshot.alwaysAllowNative`	True

Note: VMs stored on NFS datastores and configured with `snapshot.alwaysAllowNative` might encounter the `Invalid Disk Chain` error. For more information, see the VMware Knowledge Base article 89923.

Hardware Acceleration Considerations

When you use the hardware acceleration functionality with ESXi, certain considerations apply.

Several reasons might cause a hardware-accelerated operation to fail.

For any primitive that the array does not implement, the array returns an error. The error triggers the ESXi host to attempt the operation using its native methods.

The VMFS data mover does not leverage hardware offloads and instead uses software data movement when one of the following occurs:

- The source and destination VMFS datastores have different block sizes.
- The source file type is RDM and the destination file type is non-RDM (regular file).
- The source VMDK type is eagerzeroedthick and the destination VMDK type is thin.
- The source or destination VMDK is in sparse or hosted format.
- The source virtual machine has a snapshot.
- The logical address and transfer length in the requested operation are not aligned to the minimum alignment required by the storage device. All datastores created with the vSphere Client are aligned automatically.
- The VMFS has multiple LUNs or extents, and they are on different arrays.

Hardware cloning between arrays, even within the same VMFS datastore, does not work.

Storage Provisioning and Space Reclamation

vSphere supports two models of storage provisioning, thick provisioning and thin provisioning.

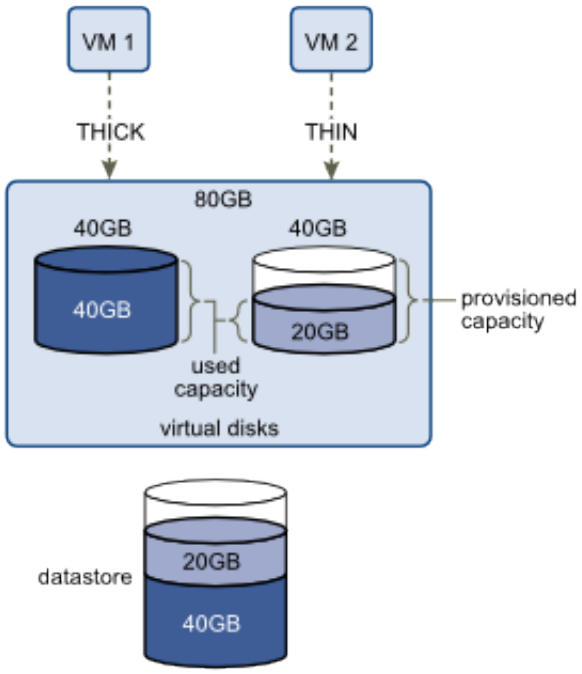
Thick provisioning	It is a traditional model of the storage provisioning. With the thick provisioning, large amount of storage space is provided in advance in anticipation of future storage needs. However, the space might remain unused causing underutilization of storage capacity.
Thin provisioning	This method contrast with thick provisioning and helps you eliminate storage underutilization problems by allocating storage space in a flexible on-demand manner. With ESXi, you can use two models of thin provisioning, array-level and virtual disk-level. Thin provisioning allows you to report more virtual storage space than there is real physical capacity. This discrepancy can lead to storage over-subscription, also called over-provisioning. When you use thin provisioning, monitor actual storage usage to avoid conditions when you run out of physical storage space.

Virtual Disk Thin Provisioning

When you create a virtual machine, a certain amount of storage space on a datastore is provisioned to virtual disk files.

By default, ESXi offers a traditional storage provisioning method for virtual machines. With this method, you first estimate how much storage the virtual machine might need for its entire life cycle. You then provision a fixed amount of storage space to the VM virtual disk in advance, for example, 40 GB. The entire provisioned space is committed to the virtual disk. A virtual disk that immediately occupies the entire provisioned space is a thick disk.

ESXi supports thin provisioning for virtual disks. With the disk-level thin provisioning feature, you can create virtual disks in a thin format. For a thin virtual disk, ESXi provisions the entire space required for the disk's current and future activities, for example 40 GB. However, the thin disk uses only as much storage space as the disk needs for its initial operations. In this example, the thin-provisioned disk occupies only 20 GB of storage. If the disk requires more space, it can expand into its entire 40 GB of provisioned space.



About Virtual Disk Provisioning Policies

When you perform certain virtual machine management operations, you can specify a provisioning policy for the virtual disk file. The operations include creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine.

NFS datastores with Hardware Acceleration and VMFS datastores support the following disk provisioning policies. On NFS datastores that do not support Hardware Acceleration, only thin format is available.

You can use Storage vMotion or cross-host Storage vMotion to transform virtual disks from one format to another.

Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand later on first write from the virtual machine. Virtual machines do not read stale data from the physical device.
Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks. Increasing the size of an Eager Zeroed Thick virtual disk causes a significant stun time for the virtual machine.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the

thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it.

Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed.

Note: If a virtual disk supports clustering solutions such as Fault Tolerance, do not make the disk thin.

Create Thin Provisioned Virtual Disks

To save storage space, you can create a virtual disk in a thin provisioned format. The thin provisioned virtual disk starts small and expands as more disk space is required. You can create thin disks only on the datastores that support disk-level thin provisioning.

This procedure assumes that you are creating a new virtual machine. For information, see the *vSphere Virtual Machine Administration* documentation.

1. Create a virtual machine.
   a) Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select **New Virtual Machine**.
   b) Select **Create a new virtual machine** and click **Next**.
   c) Follow the steps required to create a virtual machine.
2. Configure the thin virtual disk.
   a) On the Customize Hardware page, click the **Virtual Hardware** tab.
   b) Click the **New Hard disk** triangle to expand the hard disk options.
   c) Optional: Adjust the default disk size.

      With a thin virtual disk, the disk size value shows how much space is provisioned and guaranteed to the disk. At the beginning, the virtual disk might not use the entire provisioned space. The actual storage use value can be less than the size of the virtual disk.
   d) Select **Thin Provision** for Disk Provisioning.
3. Finish the virtual machine creation.

You created a virtual machine with a disk in the thin format.

If you created a virtual disk in the thin format, you can later inflate it to its full size.

View Virtual Machine Storage Resources

You can view how datastore storage space is allocated for your virtual machines.

1. Browse to the virtual machine.
2. Double-click the virtual machine and click the **Summary** tab.
3. Review the storage use information in the upper right area of the **Summary** tab.

Storage Usage shows how much datastore space is occupied by virtual machine files, including configuration and log files, snapshots, virtual disks, and so on. When the virtual machine is running, the used storage space also includes swap files.

For virtual machines with thin disks, the actual storage use value might be less than the size of the virtual disk.

Determine the Disk Format of a Virtual Machine

You can determine whether your virtual disk is in thick or thin format.

1. Right-click the virtual machine and select **Edit Settings**.
2. Click the **Virtual Hardware** tab.
3. Click the **Hard Disk** triangle to expand the hard disk options.
   The **Type** text box shows the format of your virtual disk.

If your virtual disk is in the thin format, you can inflate it to its full size.

Inflate Thin Virtual Disks

If you created a virtual disk in the thin format, you can change the format to thick.

- Make sure that the datastore where the virtual machine resides has enough space.
- Make sure that the virtual disk is thin.
- Remove snapshots.
- Power off your virtual machine.

You use the datastore browser to inflate the thin virtual disk.

1. In the vSphere Client, navigate to the folder of the virtual disk you want to inflate.
   a) Navigate to the virtual machine.
   b) Click the **Datastores** tab.
      The datastore that stores the virtual machine files is listed.
   c) Right-click the datastore and select **Browse Files**.
      The datastore browser displays contents of the datastore.
2. Expand the virtual machine folder and browse to the virtual disk file that you want to convert.
   The file has the `.vmdk` extension and is marked with the virtual disk ( ) icon.
3. Select the virtual disk file and click **Inflate**.

   Note: The option might not be available if the virtual disk is thick or when the virtual machine is running.

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Handling Datastore Over-Subscription

Because the provisioned space for thin disks can be greater than the committed space, a datastore over-subscription can occur, which results in the total provisioned space for the virtual machine disks on the datastore being greater than the actual capacity.

Over-subscription can be possible because usually not all virtual machines with thin disks need the entire provisioned datastore space simultaneously. However, if you want to avoid over-subscribing the datastore, you can set up an alarm that notifies you when the provisioned space reaches a certain threshold.

For information on setting alarms, see the *vCenter Server and Host Management* documentation.

If your virtual machines require more space, the datastore space is allocated on a first come first served basis. When the datastore runs out of space, you can add more physical storage and increase the datastore.

See Increase VMFS Datastore Capacity.

ESXi and Array Thin Provisioning

You can use thin-provisioned storage arrays with ESXi.

The ESXi host integrates with block-based storage and performs these tasks:

- The host can recognize underlying thin-provisioned LUNs and monitor their space use to avoid running out of physical space. The LUN space might change if, for example, your VMFS datastore expands or if you use Storage vMotion to migrate virtual machines to the thin-provisioned LUN. The host warns you about breaches in physical LUN space and about out-of-space conditions.
- The host can run the automatic T10 `unmap` command from VMFS6 and VM guest operating systems to reclaim unused space from the array. VMFS5 supports a manual space reclamation method.

Note: ESXi does not support enabling and disabling of thin provisioning on a storage device.

Requirements

To use the thin provisioning reporting and space reclamation features, follow these requirements:

- Use an appropriate ESXi version.

Table 228: ESXi Versions and Thin Provisioning Support

Supported thin provisioning components	ESXi 6.0 and earlier	ESXi 6.5 and later
Thin provisioning	Yes	Yes
Unmap command originating form VMFS	Manual for VMFS5. Use `esxcli storage vmfs unmap`.	Automatic for VMFS6
Unmap command originating from guest OS	Yes. Limited support.	Yes (VMFS6)

- Use storage systems that support T10-based vSphere Storage APIs - Array Integration (VAAI), including thin provisioning and space reclamation. For information, contact your storage provider and check the *VMware Compatibility Guide*.

Monitoring Space Use

The thin provision integration functionality helps you to monitor the use of space on thin-provisioned LUNs and to avoid running out of space.

The following sample flow demonstrates how the ESXi host and the storage array interact to generate breach of space and out-of-space warnings for a thin-provisioned LUN. The same mechanism applies when you use Storage vMotion to migrate virtual machines to the thin-provisioned LUN.

1. Using storage-specific tools, your storage administrator provisions a thin LUN and sets a soft threshold limit that, when reached, triggers an alert. This step is vendor-specific.
2. Using the vSphere Client, you create a VMFS datastore on the thin-provisioned LUN. The datastore spans the entire logical size that the LUN reports.
3. As the space used by the datastore increases and reaches the set soft threshold, the following actions take place:
   a. The storage array reports the breach to your host.
   b. Your host triggers a warning alarm for the datastore.
      You can contact the storage administrator to request more physical space. Alternatively, you can use Storage vMotion to evacuate your virtual machines before the LUN runs out of capacity.
4. If no space is left to allocate to the thin-provisioned LUN, the following actions take place:
   a. The storage array reports out-of-space condition to your host.

CAUTION:

In certain cases, when a LUN becomes full, it might go offline or get unmapped from the host.

b. The host pauses virtual machines and generates an out-of-space alarm.
You can resolve the permanent out-of-space condition by requesting more physical space from the storage administrator.

Identify Thin-Provisioned Storage Devices

Use the `esxcli` command to verify whether a particular storage device is thin-provisioned.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Run the `esxcli storage core device list -d=device_ID` command.

The following thin provisioning status indicates that the storage device is thin-provisioned.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXX4c
naa.XXXXXXXXXXXX4c
 Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXX4c)
 Size: 20480
 Device Type: Direct-Access
 Multipath Plugin: NMP
 ---------------------
 Thin Provisioning Status: yes
 ---------------------
```

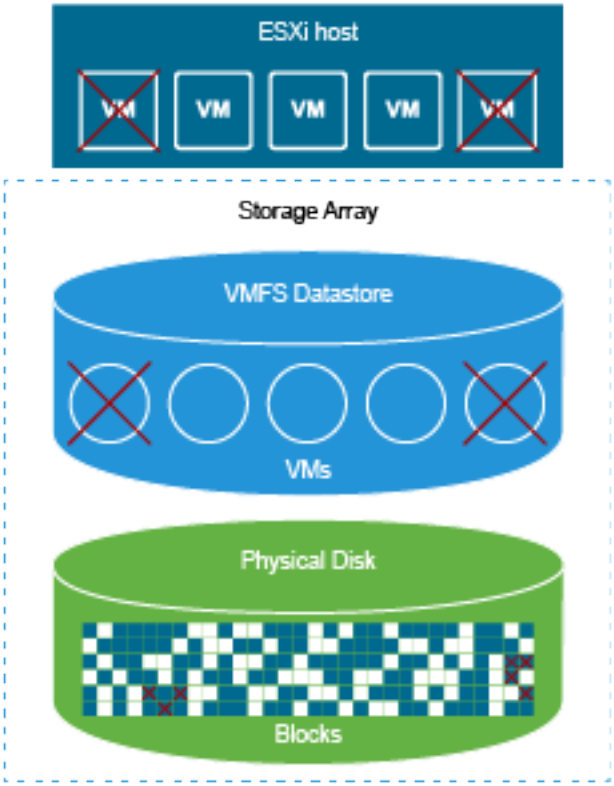
An unknown status indicates that a storage device is thick.

Note: Some storage systems present all devices as thin-provisioned no matter whether the devices are thin or thick. Their thin provisioning status is always `yes`. For details, check with your storage vendor.

Storage Space Reclamation

ESXi supports the space reclamation command, also called SCSI unmap command, that originates from a VMFS datastore or a VM guest operating system. The command helps thin-provisioned storage arrays to reclaim unused space from the VMFS datastore and thin virtual disks on the datastore. The VMFS6 datastore can send the space reclamation command automatically. With the VMFS5 datastore, you can manually reclaim storage space.

You free storage space inside the VMFS datastore when you delete or migrate the VM, consolidate a snapshot, and so on. Inside the virtual machine, storage space is freed when you delete files on the thin virtual disk. These operations leave blocks of unused space on the storage array. However, when the array is not aware that the data was deleted from the blocks, the blocks remain allocated by the array until the datastore releases them. VMFS uses the SCSI unmap command to indicate to the array that the storage blocks contain deleted data, so that the array can unallocate these blocks.



The command can also originate directly from the guest operating system. Both VMFS5 and VMFS6 datastores can provide support to the unmap command that proceeds from the guest operating system. However, the level of support is limited on VMFS5.

Depending on the type of your VMFS datastore, you use different methods to configure space reclamation for the datastore and your virtual machines.

Watch the following video to learn more about how space reclamation works.

Space Reclamation Requests from VMFS Datastores

Deleting or removing files from a VMFS datastore frees space within the file system. This free space is mapped to a storage device until the file system releases or unmaps it. ESXi supports reclamation of free space, which is also called the unmap operation.

The operation helps the storage array to reclaim unused free space. Unmapped space can be then used for other storage allocation requests and needs.

Asynchronous Reclamation of Free Space on VMFS6 Datastore

On VMFS6 datastores, ESXi supports the automatic asynchronous reclamation of free space. VMFS6 can run the unmap command to release free storage space in the background on thin-provisioned storage arrays that support unmap operations.

Asynchronous unmap processing has several advantages:

- Unmap requests are sent at a constant rate, which helps to avoid any instant load on the backing array.

- Freed regions are batched and unmapped together.
- I/O performance of other workloads is not impacted by the unmap command.

For VMFS6 datastores, you can configure the following space reclamation parameters.

Space reclamation granularity

Granularity defines the minimum size of a released space sector that underlying storage can reclaim. Storage cannot reclaim those sectors that are smaller in size than the specified granularity.

For VMFS6, reclamation granularity equals the block size. When you specify the block size as 1 MB, the granularity is also 1 MB. Storage sectors of the size smaller than 1 MB are not reclaimed.

Note: Certain storage arrays recommend an optimal unmap granularity. ESXi supports automatic unmap processing on arrays with the recommended unmap granularity of 1 MB or greater, for example 16 MB,. On the arrays with the optimal granularity of 1 MB and less, the unmap operation is supported if the granularity is a factor of 1 MB. For example, 1 MB is divisible by 512 bytes, 4 KB, 64 KB, and so on.

Space reclamation method

The method can be either priority or fixed. When the method you use is priority, you configure the priority rate. For the fixed method, you must indicate the bandwidth in MB per second.

Space reclamation priority

This parameter defines the rate at which the space reclamation operation is performed when you use the priority reclamation method. Typically, VMFS6 can send the unmap commands either in bursts or sporadically depending on the workload and configuration. For VMFS6, you can specify one of the following options.

Space Reclamation Priority	Description	Configuration
None	Disables the unmap operations for the datastore.	vSphere Client `esxcli` command
Low (default)	Sends the unmap command at a less frequent rate, 25–50 MB per second.	vSphere Client `esxcli` command
Medium	Sends the command at a rate twice faster than the low rate, 50–100 MB per second.	`esxcli` command
High	Sends the command at a rate three times faster than the low rate, over 100 MB per second.	`esxcli` command

Note: The ESXi host of version 6.5 does not recognize the medium and high priority rates. If you migrate the VMs to the host version 6.5, the rate defaults to low.

After you enable space reclamation, the VMFS6 datastore can start releasing the blocks of unused space only when it has at least one open file. This condition can be fulfilled when, for example, you power on one of the VMs on the datastore.

Manual Reclamation of Free Space on VMFS5 Datastore

VMFS5 and earlier file systems do not unmap free space automatically, but you can use the `esxcli storage vmfs unmap` command to reclaim space manually. When you use the command, be aware that it might send many unmap requests at a time. This action can lock some of the resources during the operation.

Configure Space Reclamation for a VMFS6 Datastore

When you create a VMFS6 datastore, you can modify the default parameters for automatic space reclamation.

At the VMFS6 datastore creation time, the only available method for the space reclamation is priority. To use the fixed method, edit the space reclamation settings of the existing datastore.

1. In the vSphere Client object navigator, browse to a host, a cluster, or a data center.
2. Click the **New Datastore** icon.
3. Follow the steps required to create a VMFS6 datastore.
4. On the **Partition configuration** page, specify the space reclamation parameters.

   The parameters define granularity and the priority rate at which space reclamation operations are performed. You can also use this page to disable space reclamation for the datastore.

Option	Description
Block size	The block size on a VMFS datastore defines the maximum file size and the amount of space the file occupies. VMFS6 supports the block size of 1 MB.
Space reclamation granularity	Specify granularity for the unmap operation. Unmap granularity equals the block size, which is 1 MB. Storage sectors of the size smaller than 1 MB are not reclaimed.
Space reclamation priority	Select one of the following options. • Low (default). Use the priority method for space reclamation. Enable the unmap operation at a low priority rate. • None. Select this option if you want to disable the space reclamation operations for the datastore.

   Note: In the vSphere Client, the only available settings for the space reclamation priority are Low and None. To change the settings to Medium or High, use the `esxcli` command. See Use the ESXCLI Command to Change Space Reclamation Parameters.
5. Finish the datastore creation process.

After you enable space reclamation, the VMFS6 datastore can start releasing the blocks of unused space only when it has at least one open file. This condition can be fulfilled when, for example, you power on one of the VMs on the datastore.

Change Space Reclamation Settings

When you create a VMFS6 datastore in the vSphere Client, the only method for space reclamation you can specify is the priority method. To enable the fixed method, modify the space reclamation settings for the existing datastore.

1. In the vSphere Client, navigate to the datastore.
2. Select **Edit Space Reclamation** from the right-click menu.
3. Specify the space reclamation setting.

Option	Description
Enable automatic space reclamation at fixed rate	Use the fixed method for space reclamation. Specify reclamation bandwidth in MB per second.
Disable automatic space reclamation	Deleted or unmapped blocks are not reclaimed.

4. Click **OK** to save the new settings.
5. Unmount and remount the datastore for the changes to take place.
   a) Unmount Datastores.
   b) Mount Datastores.
6. Repeat this procedure for all ESXi hosts that access the datastore.

The modified value for the space reclamation priority appears on the **General** page for the datastore.

Use the ESXCLI Command to Change Space Reclamation Parameters

You can change the default space reclamation priority, granularity, and other parameters.

1. On the ESXi host, use the following command to set space reclamation parameters.

   ```
   esxcli storage vmfs reclaim config set
   ```

   The command takes these options:

Option	Description
-b|--reclaim-bandwidth	Space reclamation fixed bandwidth in MB per second.
-g|--reclaim-granularity	Minimum granularity of automatic space reclamation in bytes.
-m|--reclaim-method	Method of automatic space reclamation. Supported options: • priority • fixed
-p|--reclaim-priority	Priority of automatic space reclamation. Supported options: • none • low • medium • high
-l|--volume-label	The label of the target VMFS volume.
-u|--volume-uuid	The uuid of the target VMFS volume.

   You can use the following examples.

   - Set the reclamation method to fixed and the rate to 100 MB per second.

     ```
     esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-method fixed -b 100
     ```

- Deactivate the VMFS automatic space reclamation.

  ```
  esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-priority none
  ```

2. Unmount the VMFS6 datastore from all other ESXi hosts where the datastore is mounted, and then remount it again.
   a) Unmount Datastores.
   b) Mount Datastores.

   This step ensures that all ESXi hosts where the VMFS6 datastore was mounted update the reclamation settings for the datastore.

Verify Settings for Automatic Space Reclamation

After you configure or edit space reclamation parameters for a VMFS6 datastore, you can review your settings.

1. In the vSphere Client, navigate to the datastore.
2. Click the **Configure** tab.
3. Click **General**, and verify the space reclamation settings.
   a) Under Properties, expand **File system** and review the value for the space reclamation granularity.
   b) Under Space Reclamation, review the setting for the space reclamation priority.

   If you configured any values through the `esxcli` command, for example, Medium or High for the space reclamation priority, these values also appear in the vSphere Client.

   #### Obtaining Parameters for VMFS6 Space Reclamation

   You can also use the `esxcli storage vmfs reclaim config get -l=VMFS_label|-u=VMFS_uuid` command to obtain information for the space reclamation configuration.

   ```
   # esxcli storage vmfs reclaim config get -l my_datastore
   Reclaim Granularity: 1048576 Bytes
   Reclaim Priority: low
   ```

Manually Reclaim Accumulated Storage Space

On VMFS datastores that do not support automatic space reclamation, you can use the `esxcli` command to reclaim unused storage space manually.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

1. To reclaim unused storage blocks on the thin-provisioned device, run the following command:

   ```
   esxcli storage vmfs unmap
   ```

   The command takes these options:

Option	Description
-l|--volume-label=*volume_label*	The label of the VMFS volume to unmap. A mandatory argument. If you specify this argument, do not use `-u|--volume-uuid=volume_uuid`.
-u|--volume-uuid=*volume_uuid*	The UUID of the VMFS volume to unmap. A mandatory argument. If you specify this argument, do not use `-l|--volume-label=volume_label`.
-n|--reclaim-unit=*number*	Number of VMFS blocks to unmap per iteration. An optional argument. If it is not specified, the command uses the default value of 200.

2. To verify whether the unmap process has finished, search for unmap in the `vmkernel.log` file.

Space Reclamation Requests from Guest Operating Systems

ESXi supports the unmap commands issued directly from a guest operating system to reclaim storage space. The level of support and requirements depend on the type of datastore where your virtual machine resides.

Inside a virtual machine, storage space is freed when, for example, you delete files on the thin virtual disk. The guest operating system notifies VMFS about freed space by sending the unmap command. The unmap command sent from the guest operating system releases space within the VMFS datastore. The command then proceeds to the array, so that the array can reclaim the freed blocks of space.

Space Reclamation for VMFS6 Virtual Machines

VMFS6 generally supports automatic space reclamation requests that generate from the guest operating systems, and passes these requests to the array. Many guest operating systems can send the unmap command and do not require any additional configuration. The guest operating systems that do not support the automatic unmaps might require user intervention. For information about guest operating systems that support the automatic space reclamation on VMFS6, contact your vendor.

Generally, the guest operating systems send the unmap commands based on the unmap granularity they advertise. For details, see documentation provided with your guest operating system.

The following considerations apply when you use space reclamation with VMFS6:

- VMFS6 processes the unmap request from the guest OS only when the space to reclaim equals 1 MB or is a multiple of 1 MB. If the space is less than 1 MB or is not aligned to 1 MB, the unmap requests are not processed.
- For VMs with snapshots in the default SEsparse format, VMFS6 supports the automatic space reclamation only on ESXi hosts version 6.7 or later.

  Space reclamation affects only the top snapshot and works when the VM is powered on.

Space Reclamation for VMFS5 Virtual Machines

Typically, the unmap command that generates from the guest operation system on VMFS5 cannot be passed directly to the array. You must run the `esxcli storage vmfs unmap` command to trigger unmaps for the array.

However, for a limited number of the guest operating systems, VMFS5 supports the automatic space reclamation requests.

To send the unmap requests from the guest operating system to the array, the virtual machine must meet the following prerequisites:

- The virtual disk must be thin-provisioned.
- Virtual machine hardware must be of version 11 (ESXi 6.0) or later.
- The advanced setting EnableBlockDelete must be set to 1.
- The guest operating system must be able to identify the virtual disk as thin.

Getting Started with Cloud Native Storage

Cloud Native Storage is a solution that provides comprehensive data management for stateful applications. When you use Cloud Native Storage, you can create the containerized stateful applications capable of surviving restarts and outages. Stateful containers leverage storage exposed by vSphere while using such primitives as standard volume, persistent volume, and dynamic provisioning.

With Cloud Native Storage, you can create persistent container volumes independent of virtual machine and container life cycle. vSphere storage backs the volumes, and you can set a storage policy directly on the volumes. After you create the

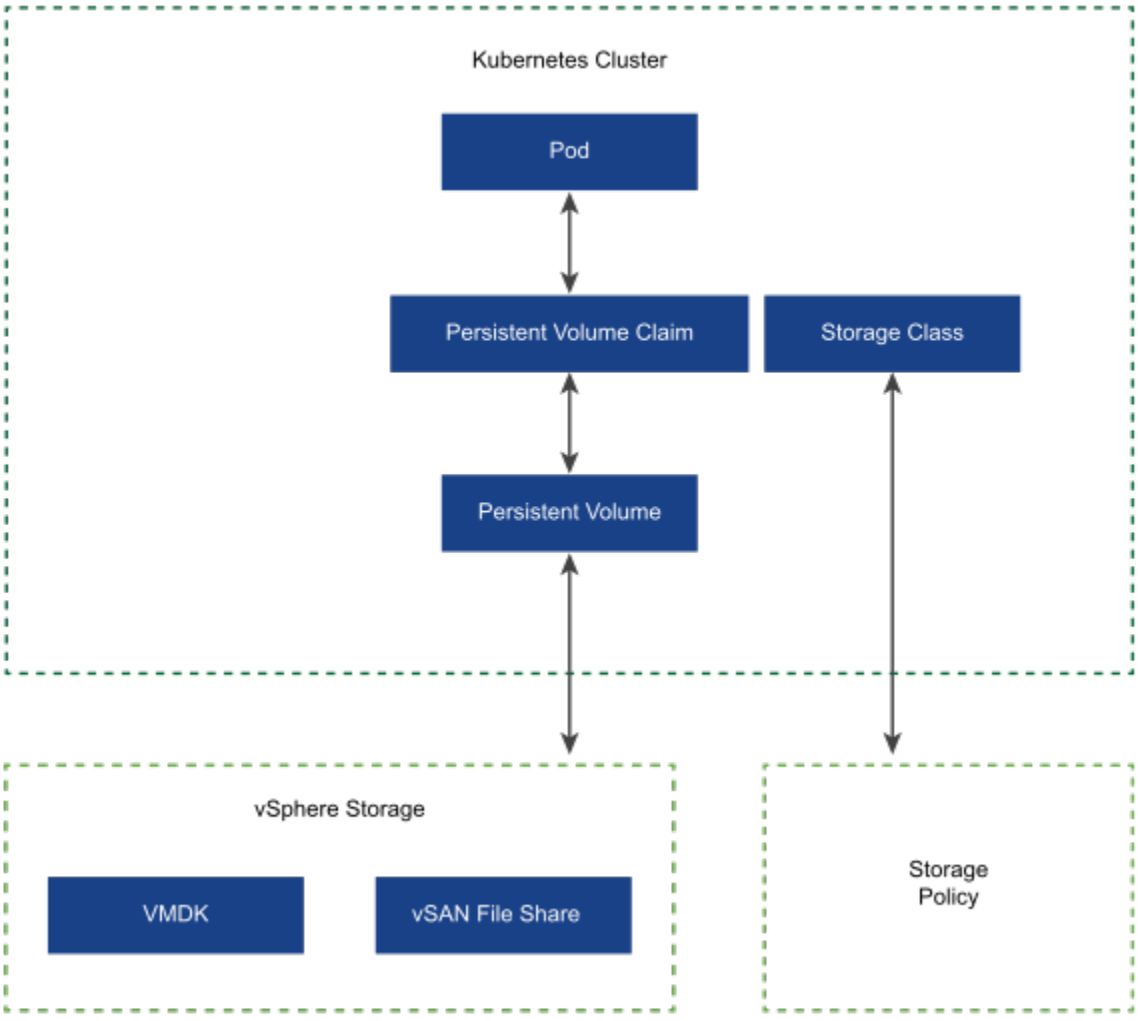
volumes, you can review them and their backing storage objects in the vSphere Client, and monitor their storage policy compliance.

vSphere Cloud Native Storage supports persistent volumes in the following Kubernetes distributions:

- Generic Kubernetes, also called vanilla, that you install from the official repositories. This *vSphere Storage* documentation covers only generic Kubernetes.
- vSphere with Tanzu. For more information, see the documentation.

Cloud Native Storage Concepts and Terminology

Be familiar with several concepts essential to the vSphere Cloud Native Storage environment.



Kubernetes Cluster

In the Cloud Native Storage environment, you can deploy a generic Kubernetes cluster in a cluster of virtual machines. On top of the Kubernetes cluster, you deploy your containerized applications. Applications can be stateful and stateless.

Note: For information on supervisor clusters and TKG clusters that you can run in vSphere with Tanzu, see the documentation.

Pod

A pod is a group of one or more containerized applications that share such resources as storage and network. Containers inside a pod are started, stopped, and replicated as a group.

Container Orchestrator

Open-source platforms, such as Kubernetes, for deployment, scaling, and management of containerized applications across clusters of hosts. The platforms provide a container-centric infrastructure.

Stateful Application

As containerized applications evolve from stateless to stateful, they require persistent storage. Unlike stateless applications that do not save data between sessions, stateful applications save data to persistent storage. The retained data is called the application's state. You can later retrieve the data and use it in the next session. Most applications are stateful. A database is as an example of a stateful application.

PersistentVolume

Stateful applications use PersistentVolumes to store their data. A PersistentVolume is a Kubernetes volume capable of retaining its state and data. It is independent of a pod and can continue to exist even when the pod is deleted or reconfigured. In the vSphere environment, the PersistentVolume objects use vSphere virtual disks of the First Class Disk (FCD) type or vSAN file shares as their backing storage. First Class Disks are also referred to as Improved Virtual Disks (IVD) or managed virtual disks.

- Virtual disks support volumes that are mounted as ReadWriteOnce. These volumes can be used only by a single Pod in Kubernetes.

  Starting with vSphere 7.0, you can use the vSphere encryption technology to protect FCD virtual disks that back persistent volumes. For more information, see Use Encryption with Cloud Native Storage.
- vSAN file shares support ReadWriteMany volumes that are mounted by many nodes. These volumes can be shared between multiple Pods or applications running across Kubernetes nodes or across Kubernetes clusters. For information about possible configurations with file shares, see Using vSAN File Service to Provision File Volumes.

StorageClass

Kubernetes uses a StorageClass to define different tiers of storage and to describe different types of requirements for storage backing the PersistentVolume. In the vSphere environment, a storage class can be linked to a storage policy. As a vSphere administrator, you create storage policies that describe different storage requirements. The VM storage policies can be used as a part of StorageClass definition for dynamic volume provisioning.

The following sample YAML file references the `Gold` storage policy that you created earlier using the vSphere Client. The resulting persistent volume VMDK is placed on a compatible datastore that satisfies the `Gold` storage policy requirements.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: gold-sc
  annotations:
    storageclass.kubernetes.io/is-default-class:
 "true"
provisioner: csi.vsphere.vmware.com
```

```
parameters:
  storagepolicyname: "Gold"
```

PersistentVolumeClaim

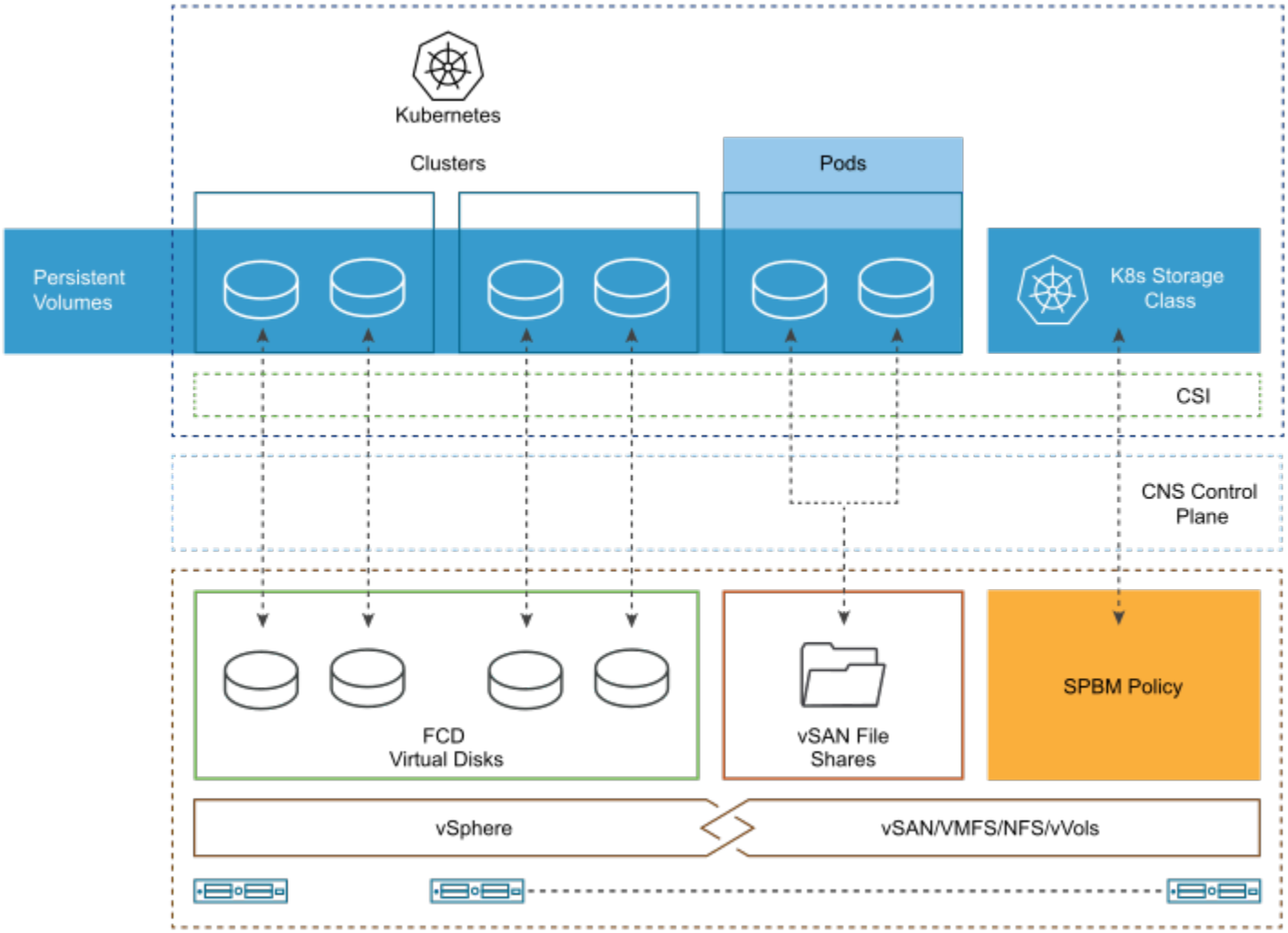
Typically, applications or pods can request persistent storage through a PersistentVolumeClaim. The PersistentVolumeClaim specifies the type and class of storage, the access mode, either ReadWriteOnce or ReadWriteMany, and other parameters for the PersistentVolume. The request can then dynamically provision the corresponding PersistentVolume object and the underlying virtual disk or vSAN file share in the vSphere environment.
Once the claim is created, the PersistentVolume is automatically bound to the claim. Pods use the claim to mount the PersistentVolume and access storage.
When you delete this claim, the corresponding PersistentVolume object and the underlying storage are deleted.

```
kind: PersistentVolumeClaim
metadata:
 name: persistent-VMDK
spec:
 accessModes:
 - ReadWriteOnce
 resources:
 requests:
 storage: 5Gi
 storageClassName: gold-sc
```

Cloud Native Storage Components

Cloud Native Storage uses several components to integrate with vSphere storage.

The following illustration shows how these components interact.



Kubernetes Cluster

In the Cloud Native Storage environment, a generic Kubernetes cluster is deployed on a cluster of virtual machines, or nodes, that run in vSphere. A Kubernetes user directly interacts with the cluster when deploying stateful applications on top of it.

Container Storage Interface (CSI) for vSphere

To consume underlying infrastructure resources, the cluster requires a CSI driver.

The vSphere CSI is an out-of-tree plug-in that exposes vSphere storage to containerized workloads on container orchestrators, such as Kubernetes. The plug-in enables vSAN and other types of vSphere storage.

The vSphere CSI communicates with the CNS control plane on vCenter Server for all storage provisioning operations. The vSphere CSI supports the following functionalities:

- Dynamic provisioning of container volumes.
- The vSphere First Class Disk functionality.
- Kubernetes zones.
- Conventional and raw mounts.
- Single vCenter Server, and multiple data centers and clusters.
- Provisioning from multiple datastores or datastore clusters.

	• vSAN File Service On Kubernetes, the CSI driver is used with the out-of-tree vSphere Cloud Provider Interface (CPI). The CSI driver is shipped as a container image and must be deployed by the cluster administrator. For information, *vSphere Container Storage Plug-in Deployment* section of the *Getting Started with VMware vSphere Container Storage Plug-in* documentation.
Cloud Native Storage Server Component	The CNS server component, or the CNS control plane, resides in vCenter Server. It is an extension of vCenter Server management that implements the provisioning and life cycle operations for the container volumes. When provisioning container volumes, it interacts with vCenter Server to create storage objects that back the volumes. The Storage Policy Based Management functionality guarantees a required level of service to the volumes. The CNS also performs query operations that allow you to manage and monitor container volumes and their backing storage objects through vCenter Server.
First Class Disk (FCD)	Also called Improved Virtual Disk (IVD) or managed virtual disk. It is a named virtual disk unassociated with a VM. These disks reside on a vSAN, VMFS, NFS, or vVols datastore and back ReadWriteOnce container volumes. The FCD technology allows to perform life cycle operations related to persistent volumes outside of the VM or pod life cycle. If the VM is a Kubernetes node that runs multiple container based applications and uses persistent volumes and virtual disks for many applications, CNS facilitates life cycle operations at the container and persistent volume granularity.
vSAN File Service	It is a vSAN layer that provides file shares. Currently, it supports NFSv3 and NFSv4.1 file shares. Cloud Native Storage uses vSAN file shares for persistent volumes of the ReadWriteMany type. A single ReadWriteMany volume can be mounted by multiple nodes. The volume can be shared between multiple pods or applications running across Kubernetes nodes or across Kubernetes clusters.
Storage Policy Based Management	Storage Policy Based Management is a vCenter Server service that supports provisioning of persistent volumes according to specified storage requirements. After provisioning, the service monitors compliance of the volume with the required policy characteristics.

Using vSAN File Service to Provision File Volumes

vSAN file service offers vSAN file shares that are consumed by persistent volumes of the ReadWriteMany (RWM) type. A single RWM volume can be mounted by multiple nodes. The volume can be shared between multiple pods or applications running across Kubernetes nodes or across Kubernetes clusters.

When a Kubernetes pod request an RWM volume, Cloud Native Storage communicates with vSAN file service to create an NFS-based file share of the requested size and storage class. Cloud Native Storage then mounts the RWM volume into the Kubernetes worker node where the pod runs. If multiple nodes are requesting access to the RWM volume, Cloud Native Storage determines that the RWM volume already exists for that particular deployment and mounts the existing volume into the nodes.

To be able to support RWM volumes, your environment must include the following items.

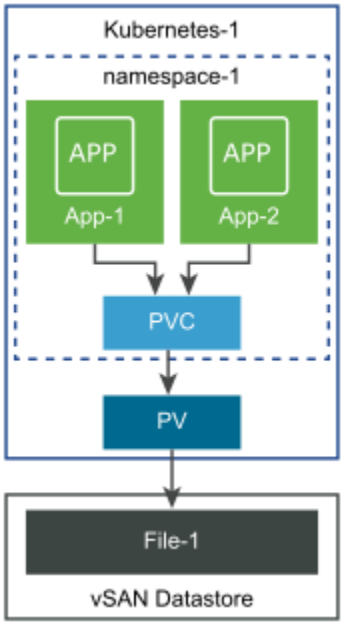
- vSphere 7.0 and later with vSAN

- vSAN file service enabled. For information, see the *Administering VMware vSAN* documentation.
- Kubernetes version 1.14 and later
- Compatible version of CSI. For information, see the *Getting Started with VMware vSphere Container Storage Plug-in* documentation.

You can use different configurations for file volumes.

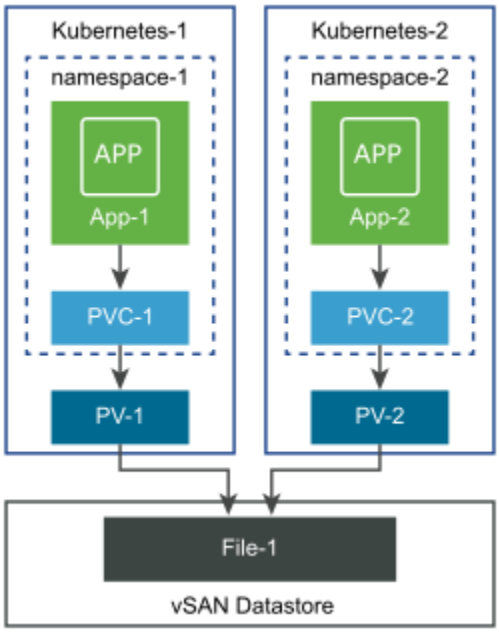
Single File Volume Shared Across Applications in the Same Namespace

In this example, a single file volume is used as shared storage across different applications in the same namespace. You use a single persistent volume claim to provision the file volume.



Single File Volume Shared Across Applications and Namespaces

This example uses a single file volume as shared storage across different applications and different namespaces. For each namespace, you create a separate persistent volume claim to provision the same file volume.



Cloud Native Storage Users

The types of users involved in the process of creating and monitoring Kubernetes volumes in the vSphere Cloud Native Storage environment generally fall into two categories, a Kubernetes user and a vSphere administrator. Both types of users have access to different tools and perform different tasks.

CNS Kubernetes User

The Kubernetes user might be a Kubernetes developer and an application owner, a Kubernetes administrator, or combine functions of both. The tasks that the Kubernetes user performs in the Cloud Native Storage environment include the following:

- Deploy and manage the vSphere CSI. For information, see the vSphere Container Storage Plug-in Deployment section of the Getting Started with VMware vSphere Container Storage Plug-in documentation.
- Provision persistent volumes. For information about block volumes, see vSphere CSI Driver - Block Volume. For information about file volumes, see vSphere CSI Driver - File Volume.
- Perform life cycle operations for persistent volumes.
- Perform life cycle operations for storage classes.

CNS vSphere User

A CNS vSphere user, or a vSphere administrator, has access to the vSphere Client to perform the following tasks:

- Perform life cycle operations for the VM storage policies. For example, create a VM storage policy to be used for a Kubernetes storage class and communicate its name to the Kubernetes user. See Create a Storage Policy for Kubernetes.
- Use the Cloud Native Storage section of the vSphere Client to monitor health and storage policy compliance of the container volumes across the Kubernetes clusters. See Monitor Container Volumes Across Kubernetes Clusters.

Cloud Native Storage for vSphere Administrators

A vSphere administrator delivers storage resources to the Kubernetes team and creates VM storage policies that describe different storage requirements and classes of services. After the Kubernetes workloads with persistent storage are provisioned, the vSphere administrator can monitor the life cycle of the backing storage resources and their compliance to the requirements.

Requirements of Cloud Native Storage

Your Cloud Native Storage environment and virtual machines that participate in the Kubernetes cluster must meet several requirements.

Cloud Native Storage Requirements

- vSphere 6.7 Update 3 or later.
- A compatible version of Kubernetes.
- A Kubernetes cluster deployed on the virtual machines. For details about deploying the vSphere CSI plug-in and running the Kubernetes cluster on vSphere, see the Driver Deployment documentation in GitHub.

Requirements for Kubernetes Cluster Virtual Machines

- Virtual machines with hardware version 15 or later. Install VMware Tools on each node virtual machine.
- Virtual machine hardware recommendations:
  - Set CPU and memory adequately based on workload requirements.
  - Use the VMware Paravirtual SCSI controller for the primary disk on the Node VM.
- All virtual machines must have access to a shared datastore, such as vSAN.
- Set the `disk.EnableUUID` parameter on each node VM. See Configure Kubernetes Cluster Virtual Machines.
- To avoid errors and unpredictable behavior, do not take snapshots of CNS node VMs.

Requirements for CNS File Volume

- Use vSphere version 7.0 or later with a compatible Kubernetes version.
- Use a compatible version of CSI. For information, see the Kubernetes vSphere CSI Driver documentation on GitHub.
- Enable and configure the vSAN file service. You must configure the necessary file service domains, IP pools, network, and so on. For information, see the *Administering VMware vSAN* documentation.
- Follow specific guidelines to configure network access from a guest OS in the Kubernetes node to a vSAN file share. See Configuring Network Access to vSAN File Share.

Configuring Network Access to vSAN File Share

To be able to provision ReadWriteMany persistent volumes in your generic vSphere Kubernetes environment, configure necessary networks, switches, and routers from the Kubernetes nodes to the vSAN file service network.

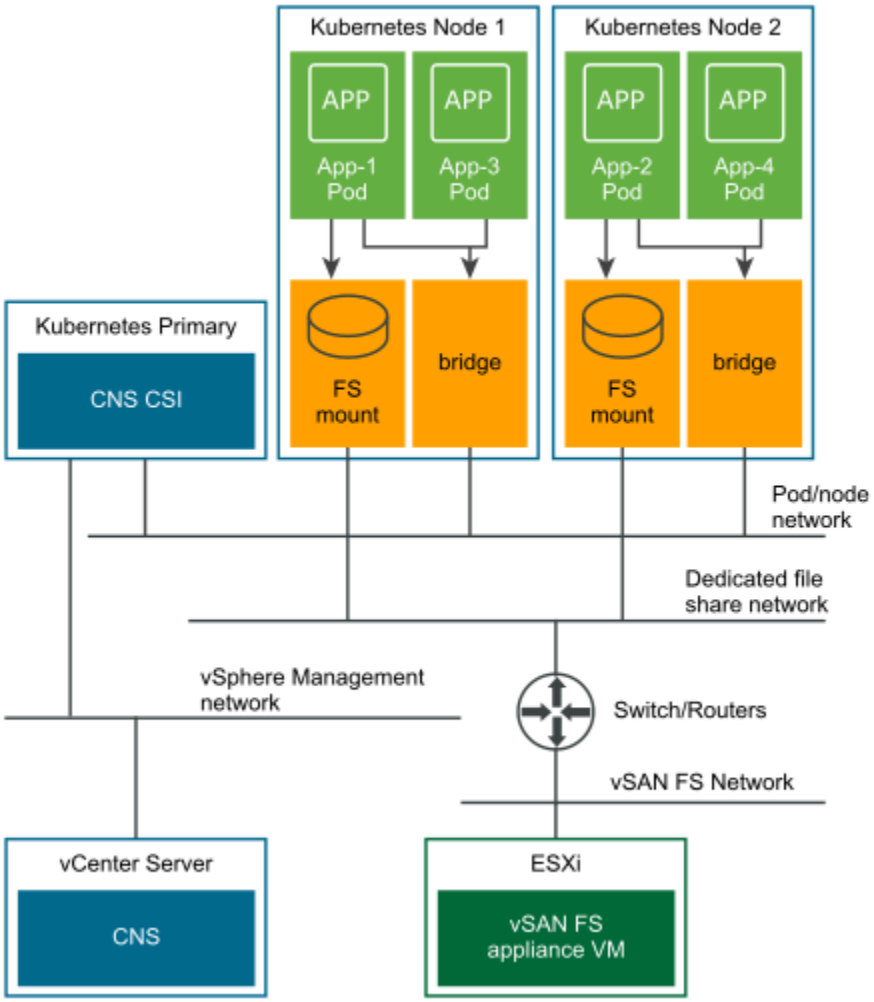
Setting Up Network

When configuring the networks, follow these requirements:

- On every Kubernetes node, you can use a dedicated vNIC for the vSAN file share traffic. This option is required only if you want to use a secure data traffic path for your file volumes.

- If you use a dedicated vNIC, make sure that the traffic through the dedicated vNIC is routable to one or many vSAN file service networks.
- Make sure that only the guest OS on each Kubernetes node can directly access the vSAN file share through the file share IP address. The pods in the node cannot ping or access the vSAN file share by its IP address.
  CNS CSI driver ensures that only those pods that are configured to use the CNS file volume can access the vSAN file share by creating a mount point in the guest OS.
- Avoid creating an IP address clash between the node VMs and vSAN file shares.

The following illustration is an example of the CNS network configuration with the vSAN file share service.



In the illustration, the sample networking configuration follows these guidelines.

- The configuration uses separate networks for different items in the CNS environment.

Network	Description
vSphere management network	Typically, in a generic Kubernetes cluster, every node has access to this network.
Pod or node network	Kubernetes uses this network for the node to node or pod to pod communication.
Dedicated file share network	CNS file volume data traffic uses this network.

Network	Description
vSAN file share network	Network where the vSAN file share is enabled and where file shares are available.

- Every Kubernetes node has a dedicated vNIC for the file traffic. This vNIC is separate from the vNIC used for the node to node or pod to pod communication. This configuration is used only as an example, but is not mandatory.
- Only those applications that are configured to use the CNS file share have access to vSAN file shares through the mount point in the node guest OS. For example, in the illustration, the following takes place:
  - App-1 and App-2 pods are configured to use a file volume, and have access to the file share through the mount point created by the CSI driver.
  - App-3 and App-4 are not configured with a file volume and cannot access file shares.
- The vSAN file shares are deployed as containers in a vSAN file share appliance VM on the ESXi host. A Kubernetes deployer, which is a software or service that can configure, deploy, and manage Kubernetes clusters, configures necessary routers and switches, so that the guest OS in the Kubernetes node can access the vSAN file shares.

Security Limitations

Although the dedicated vNIC prevents an unauthorized pod from accessing the file shares directly, certain security limitations exist:

- The CNS file functionality assumes that anyone who has the CNS file volume ID is an authorized user of the volume. Any user that has the CNS file volume ID can access the data stored in the volume.
- CNS file volume supports only the AUTH_SYS authentication, which is a user ID-based authentication. To protect access to the data in the CNS file volume, you must use appropriate user IDs for the containers accessing the CNS file volume.
- An unbound ReadWriteMany persistent volume referring to a CNS file volume can be bound by a persistent volume claim created by any Kubernetes user under any namespace. Make sure that only authorized users have access to Kubernetes to avoid security issues.

Configuring the CSI Driver to Access vSAN File Service Clusters

Depending on the configuration, the CSI driver can provision file volumes on one or several vSAN clusters where the file service is enabled.

You can restrict access to only specific vSAN clusters where the file service is enabled. When deploying the Kubernetes cluster, configure the CSI driver with access to specific file service vSAN clusters. As a result, the CSI driver can provision the file volumes only on those vSAN clusters.

In the default configuration, the CSI driver uses any file service vSAN cluster available in vCenter Server for the file volume provisioning. The CSI driver does not verify which file service vSAN cluster is accessible while provisioning file volumes.

Cloud Native Storage Roles and Privileges

The CNS vSphere user must have specific privileges to perform operations related to Cloud Native Storage.

You can create several roles to assign sets of permissions on the objects that participate in the Cloud Native Storage environment.

Note: These roles need to be created only for generic Kubernetes clusters. If you work in the vSphere with Tanzu environment, use the Workload Storage Manager role for storage operations.

For more information about roles and permissions in vSphere, and how to create a role, see the *vSphere Security* documentation.

Role Name	Privilege Name	Description	Required On
CNS-Datastore	Datastore > Low level file operations	Allows performing read, write, delete, and rename operations in the datastore browser.	Shared datastore where persistent volumes reside.
CNS-HOST-CONFIG-STORAGE	Host > Configuration > Storage partition configuration	Allows vSAN datastore management.	Required on a vSAN cluster with vSAN file service. Required for file volume only.
CNS-VM	Virtual machine > Change Configuration > Add existing disk	Allows adding an existing virtual disk to a virtual machine.	All cluster node VMs.
	Virtual Machine > Change Configuration > Add or remove device	Allows addition or removal of any non-disk device.	
CNS-SEARCH-AND-SPBM	CNS > Searchable	Allows storage administrator to see Cloud Native Storage UI.	Root vCenter Server.
	Profile-driven storage > Profile-driven storage view	Allows viewing of defined storage policies.	
Read-only	Default role	Users with the Read Only role for an object are allowed to view the state of the object and details about the object. For example, users with this role can find the shared datastore accessible to all node VMs. For zone and topology-aware environments, all ancestors of node VMs, such as a host, cluster, and data center must have the Read-only role set for the vSphere user configured to use the CSI driver and CCM. This is required to allow reading tags and categories to prepare the nodes' topology.	All hosts where the nodes VMs reside Data center

Create a Storage Policy for Kubernetes

The vSphere storage object that will back a Kubernetes containerized application needs to meet specific storage requirements. As a vSphere user, you create a VM storage policy based on the requirements provided to you by the Kubernetes user.

- The Kubernetes user identifies the Kubernetes cluster where the stateful containerized application will be deployed.
- The Kubernetes user collects storage requirements for the containerized application and communicates them to the vSphere user.
- Required privileges: **VM storage policies** > **Update** and **VM storage policies** > **View**.

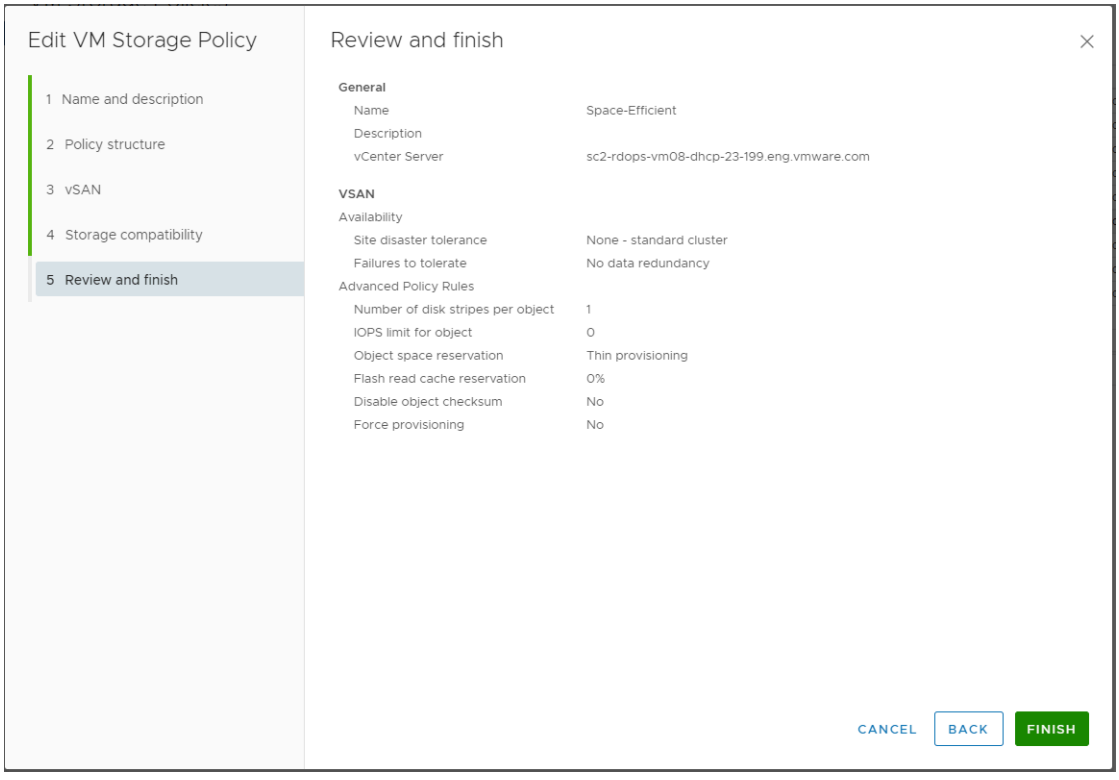
The storage policy will be associated with the virtual disk or vSAN file share that back the Kubenetes container.

If you have multiple vCenter Server instances in your environment, create the VM storage policy on each instance. Use the same policy name across all instances.

1. In the vSphere Client, open the **Create VM Storage Policy** wizard.
   a) Click **Menu** > **Policies and Profiles**.
   b) Under **Policies and Profiles**, click **VM Storage Policies**.
   c) Click **Create**.
2. Enter the policy name and description, and click **Next**.

Option	Action
vCenter Server	Select the vCenter Server instance.
Name	Enter the name of the storage policy, for example `Space-Efficient`.
Description	Enter the description of the storage policy.

3. On the **Policy structure** page under Datastore-specific rules, select **Enable rules for vSAN storage** and click **Next**.
4. On the **vSAN** page, define the policy rule set and click **Next**.
   a) On the **Availability** tab, define the **Site disaster tolerance** and **Failures to tolerate**.
   b) On the **Advanced Policy Rules** tab, define advanced policy rules, such as number of disk stripes per object and flash read cache reservation.
5. On the **Storage compatibility** page, review the list of vSAN datastores that match this policy and click **Next**.
6. On the **Review and finish** page, review the policy settings, and click **Finish**.



You can now inform the Kubernetes user of the storage policy name. The VM storage policy you created will be used as a part of storage class definition for dynamic volume provisioning.

Configure Kubernetes Cluster Virtual Machines

On each node VM, enable the disk.EnableUUID parameter, so that the VMs can successfully mount the virtual disks.

- Create several VMs for your Kubernetes cluster. For the VM requirements, see Requirements of Cloud Native Storage.
- Required privilege: **Virtual machine** > **Configuration** > **Settings**.

Note: To avoid errors and unpredictable behavior, do not take snapshots of CNS node VMs.

Perform these steps for each of the VM nodes that participate in the cluster.

1. In the vSphere Client, right-click the virtual machine and select **Edit Settings**.
2. Click the **VM Options** tab and expand the **Advanced** menu.
3. Click **Edit Configuration** next to Configuration Parameters.
4. Configure the `disk.EnableUUID` parameter.

   If the parameter exists, make sure that its value is set to True. If the parameter is not present, add it and set its value to True.

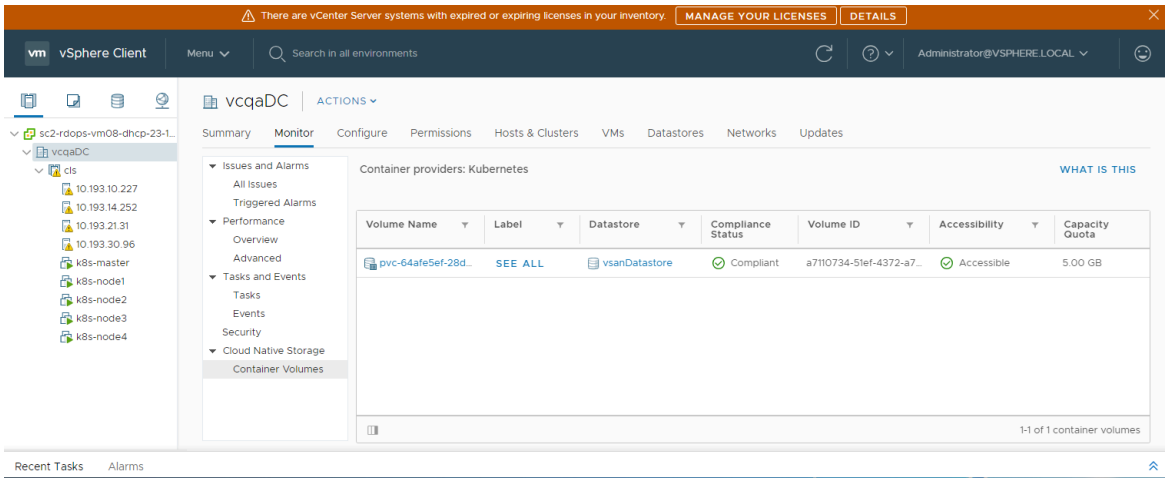
Name	Value
`disk.EnableUUID`	True

Monitor Container Volumes Across Kubernetes Clusters

After a stateful application gets deployed in Kubernetes, the volumes and their backing vSphere storage objects become visible in the vSphere Client. You can display and monitor the volumes and troubleshoot any potential storage issues.

Note: If you experience failures on the Kubernetes CNS server, the CNS objects in the vSphere Client might not display correctly until full synchronization takes place.

1. Navigate to the vCenter Server instance, a data center, or a datastore.
2. Click the **Monitor** tab and click **Container Volumes** under **Cloud Native Storage**.
3. Observe the container volumes available in your environment and monitor their storage policy compliance status.

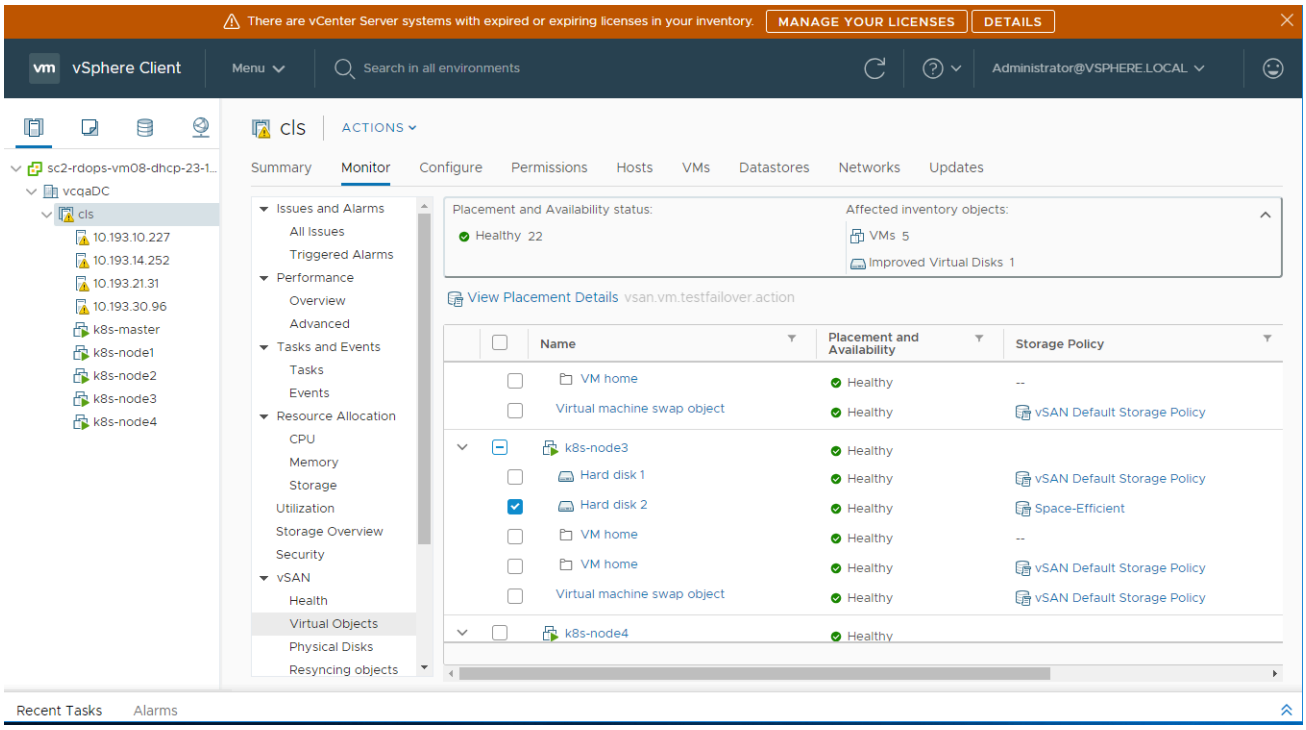


4. Click the **SEE ALL** link in the Label column to view additional details.

   The details include the name of the PersistentVolumeClaim, StorageClass, and so on, and help you map the volume to the Kubernetes objects associated with it.

5. Click the link in the **Volume Name** column to review various components that back the volume and such details as placement, compliance, and storage policy.

   Note: The **Virtual Objects** screen is available only when the underlying datastore is vSAN.



Use Encryption with Cloud Native Storage

Starting with vSphere 7.0, you can use the vSphere encryption technology to protect FCD virtual disks that back persistent volumes.

Using encryption in your vSphere environment requires some preparation, and includes setting up a trusted connection between vCenter Server and a key provider. vCenter Server can then retrieve keys from the key provider as needed. For information about components that participate in the vSphere encryption process, see vSphere Virtual Machine Encryption Components in the *vSphere Security* documentation.

1. Set up the key provider in your vSphere environment.

   For information, see Set up the Key Management Server Cluster.

2. Encrypt all node VMs on the Kubernetes cluster.

   Use the vSphere Client to perform this step.

   a) Navigate to a node VM.
   b) From the right-click menu, select **VM Policies** > **Edit VM Storage Policies**.
   c) From the **VM storage policy** drop-down menu, select **VM Encryption Policy** and click **OK**.

      To expedite the encryption process of the node VMs, you can encrypt only the VM home.

3. Create encrypted persistent volumes in the Kubernetes cluster with the vSphere CSI setup.

   a) Create a StorageClass that references the VM Encryption Storage Policy.

      Use the following YAML file as an example.

```
kind: StorageClass
```

```
apiVersion: storage.k8s.io/v1
metadata:
  name: encryption
provisioner: csi.vsphere.vmware.com
parameters:
  storagePolicyName: "VM Encryption Policy"
  datastore: vsanDatastore
```

b) Use the PersistentVolumeClaim to provision the persistent volume.

The PersistentVolumeClaim must include the name of the encryption storage class in the `storageClassName` field.

Migrating Container Volumes in vSphere

vSphere Cloud Native Storage supports migration of persistent container volumes between datastores.

Considerations and Limitations

When you perform the migration, keep in mind the following considerations:

- You can migrate only single block volumes.
- Make sure that original and target datastores are accessible to all nodes of the Kubernetes cluster. This applies to single zone deployments and to Kubernetes clusters deployed across multiple zones.
- If a volume is attached to a VM, the VM remains locked during volume relocation. If the volume you relocate is attached to a node VM, the system does not allow any other control operations on the VM. The operations include attaching or detaching other volumes to the VM, migrating the VM to a different datastore, changing any configuration of the VM, and so on.
- Cloud Native Storage does not support PMEM storage. Attempts to relocate a volume to a PMEM datastore fail.
- The target datastore must have sufficient free capacity to accommodate the migrated volume. If the free space of a datastore is less than the volume size, you cannot select the datastore for migration.
- The vSphere Client does not support automatic storage policy changes during the migration operation. However, the system doesn't prevent you from selecting a datastore with incompatible policy as a target datastore for migration.
- After the migration, you can locate the virtual disk that backs the volume in one of the following folders on a target datastore:
  - FCD directory on the datastore.
  - VM folder if the volume is attached to a VM.

For additional details, see the VMware Knowledge Base article 90607.

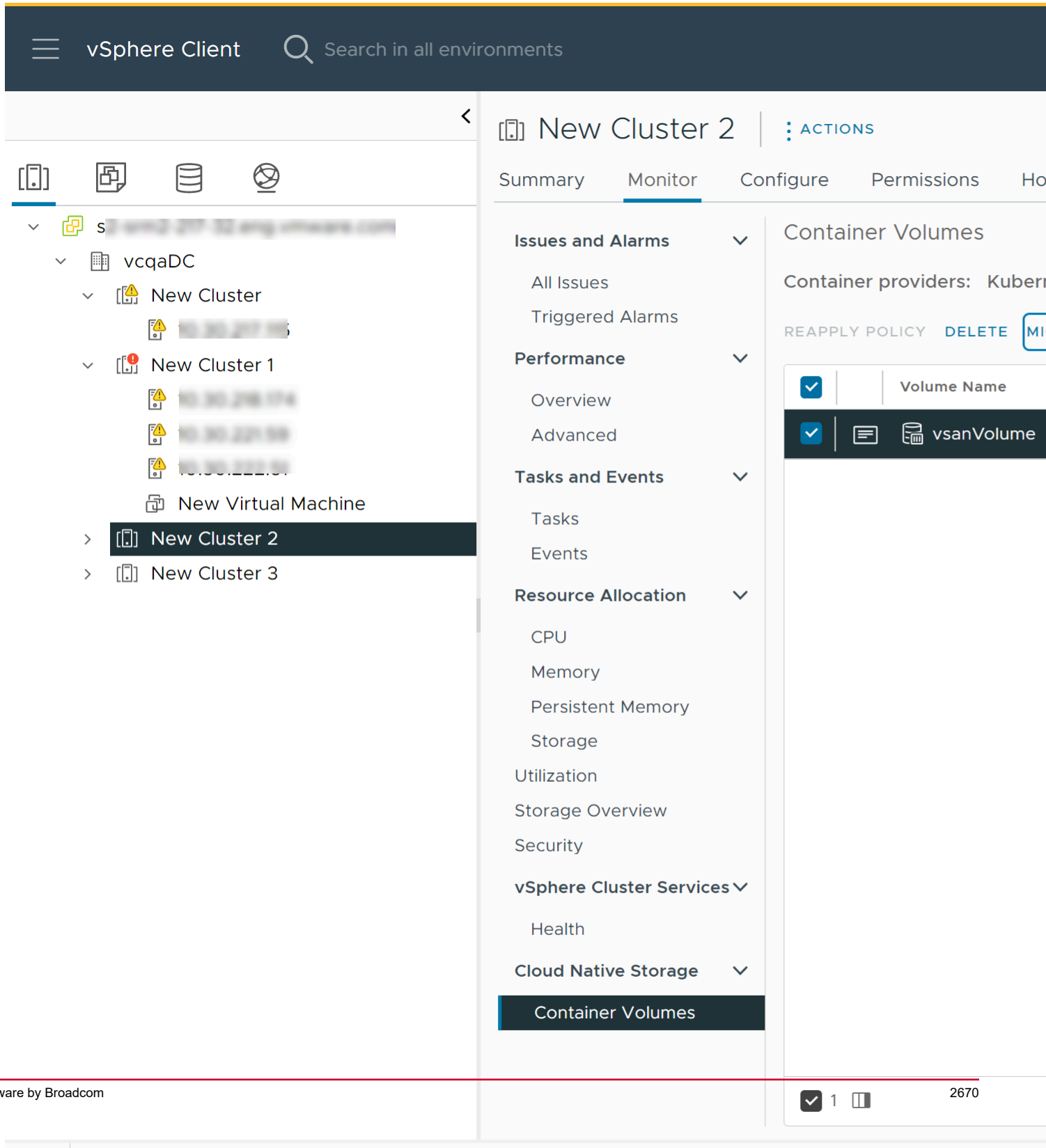
Migrate Container Volumes

You can use the vSphere Client to migrate the persistent container volumes.

- Make sure that the target datastore has sufficient free capacity to accommodate the migrated volume.

- Make sure you have permissions for the target datastore.

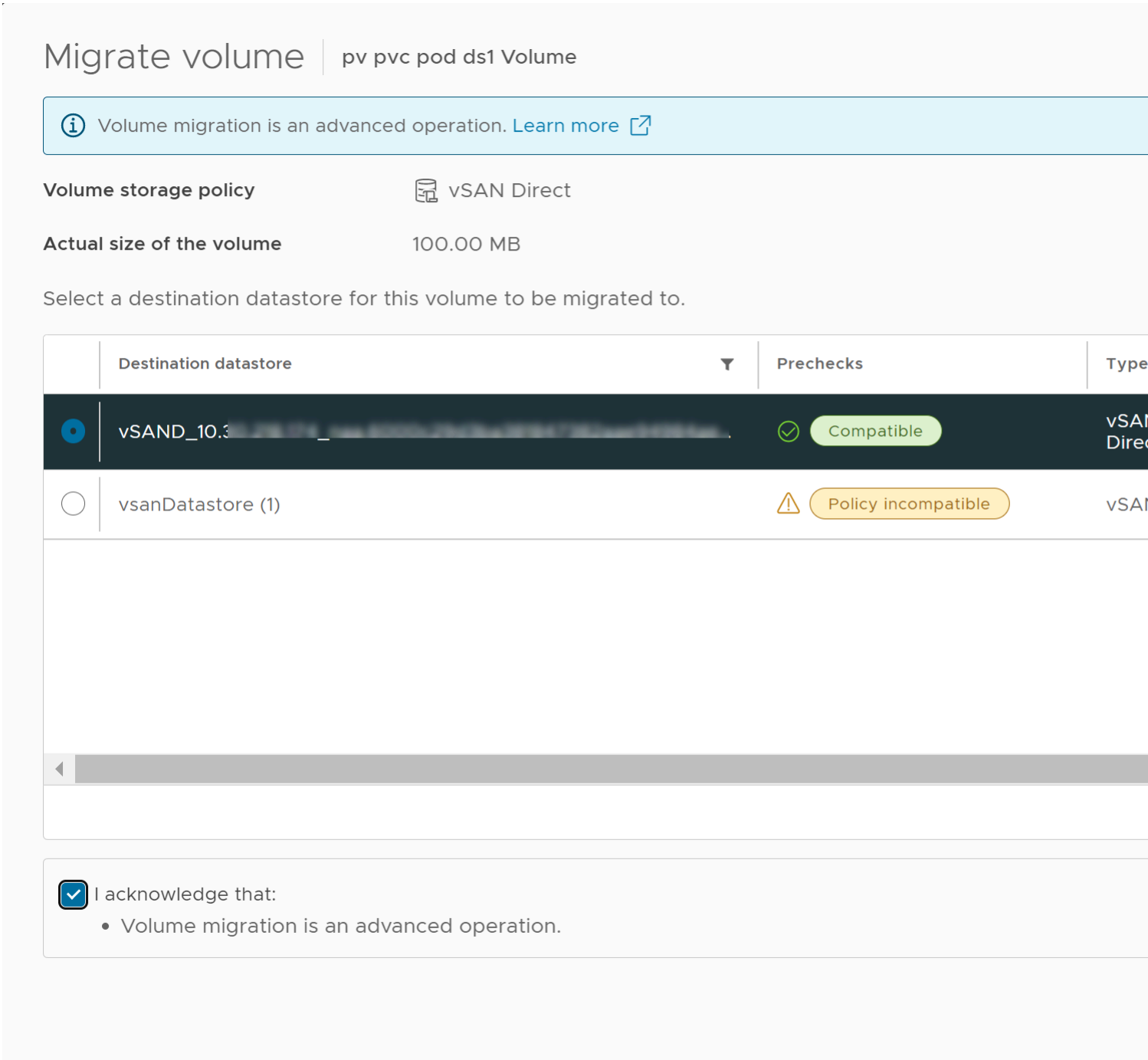
1. Navigate to the vCenter Server instance, a data center, a datastore, or a cluster.
2. Click the **Monitor** tab and click **Container Volumes** under **Cloud Native Storage**.
3. From the list of volumes, select a volume and click **Migrate**.



4. On the **Migrate volume** page, select the target datastore.

   The target datastore might display a warning. You can still proceed with the migration operation when the warnings include the following:

   - Policy incompatible. When the storage policy of the target datastore is not the same as the storage policy of the volume.
   - Inaccessible volume. When the volume is migrated from a datastore that is accessible from a set of hosts to a datastore that is not accessible from all hosts.



5. Select the **Acknowledge** check box and click **Migrate** to proceed with the migration operation.

Using vmkfstools

`vmkfstools` is one of the ESXi Shell commands for managing VMFS volumes, storage devices, and virtual disks. You can perform many storage operations using the `vmkfstools` command. For example, you can create and manage VMFS datastores on a physical partition, or manipulate virtual disk files, stored on VMFS or NFS datastores.

Note: After you make a change using the `vmkfstools` , the vSphere Client might not be updated immediately. Use a refresh or rescan operation from the client.

For more information on the ESXi Shell, see *Getting Started with ESXCLI*.

vmkfstools Command Syntax

Generally, you do not need to log in as the root user to run the `vmkfstools` commands. However, some commands, such as the file system commands, might require the root user login.

The `vmkfstools` command supports the following command syntax:

`vmkfstools`*`options target`*.

Target specifies a partition, device, or path to apply the command option to.

Table 229: `vmkfstools` Command Arguments

Argument	Description
options	One or more command-line options and associated arguments that you use to specify the activity for `vmkfstools` to perform. For example, selecting the disk format when creating a new virtual disk. After entering the option, specify a target on which to perform the operation. Target can indicate a partition, device, or path.
partition	Specifies disk partitions. This argument uses a *`disk_ID:P`* format, where *`disk_ID`* is the device ID returned by the storage array and *`P`* is an integer that represents the partition number. The partition digit must be greater than zero (0) and must correspond to a valid VMFS partition.
device	Specifies devices or logical volumes. This argument uses a path name in the ESXi device file system. The path name begins with `/vmfs/devices` , which is the mount point of the device file system. Use the following formats when you specify different types of devices: • `/vmfs/devices/disks` for local or SAN-based disks. • `/vmfs/devices/lvm` for ESXi logical volumes. • `/vmfs/devices/generic` for generic SCSI devices.
path	Specifies a VMFS file system or file. This argument is an absolute or relative path that names a directory symbolic link, a raw device mapping, or a file under `/vmfs` . • To specify a VMFS file system, use this format: `/vmfs/volumes/`*`file_system_UUID`* or `/vmfs/volumes/`*`file_system_label`* • To specify a file on a VMFS datastore, use this format: `/vmfs/volumes/`*`file_system_label`*`|`*`file_system_UUID`*`/[dir]/myDisk.vmdk` If the current working directory is the parent directory of `myDisk.vmdk`, do not enter the entire path.

The vmkfstools Command Options

The `vmkfstools` command has several options. Some of the options are suggested for advanced users only.

The long and single-letter forms of the options are equivalent. For example, the following commands are identical.

```
vmkfstools --createfs vmfs6 --blocksize 1m disk_ID:P
vmkfstools -C vmfs6 -b 1m disk_ID:P
```

-v Suboption

The `-v` suboption indicates the verbosity level of the command output.

The format for this suboption is as follows:

```
-v --verbose number
```

You specify the *number* value as an integer from 1 through 10.

You can specify the `-v` suboption with any `vmkfstools` option. If the output of the option is not suitable for use with the `-v` suboption, `vmkfstools` ignores `-v` .

Note: Because you can include the `-v` suboption in any `vmkfstools` command line, `-v` is not included as a suboption in the option descriptions.

File System Options

File system options allow you to create and manage VMFS datastores. These options do not apply to NFS. You can perform many of these tasks through the vSphere Client.

Listing Attributes of a VMFS Datastore

Use the `vmkfstools` command to list attributes of a VMFS datastore.

```
-P|--queryfs
      -h|--humanreadable
```

When you use this option on any file or directory that resides on a VMFS datastore, the option lists the attributes of the specified datastore. The listed attributes typically include the file system label, the number of extents for the datastore, the UUID, and a list of the devices where each extent resides.

Note: If any device backing VMFS file system goes offline, the number of extents and available space change accordingly.

You can specify the `-h|--humanreadable` suboption with the `-P` option. If you do so, `vmkfstools` lists the capacity of the volume in a more readable form.

Example of Listing VMFS Attributes

```
~ vmkfstools -P -h /vmfs/volumes/my_vmfs
VMFS-5.81 (Raw Major Version: 14) file system spanning 1 partitions.
File system label (if any): my_vmfs
Mode: public
Capacity 99.8 GB, 97.5 GB available, file block size 1 MB, max supported file size 62.9 TB
UUID: 571fe2fb-ec4b8d6c-d375-XXXXXXXXXXXX
Partitions spanned (on "lvm"):
        eui.3863316131XXXXXX:1
Is Native Snapshot Capable: YES
```

Creating a VMFS Datastore or a Scratch Partition

Use the `vmkfstools` command to create a VMFS datastore or a scratch partition.

```
-C|--createfs [vmfs5|vmfs6|vfat]
```

This option creates the VMFS datastore on the specified SCSI partition, such as *`disk_ID:P`*. The partition becomes the head partition of the datastore. For VMFS5 and VMFS6, the only available block size is 1 MB.

You can specify the following suboptions with the `-C` option.

- `-S|--setfsname` - Define the volume label of the VMFS datastore you are creating. Use this suboption only with the `-C` option. The label you specify can be up to 128 characters long and cannot contain any leading or trailing blank spaces.
  Note: vCenter Server supports the 80 character limit for all its entities. If a datastore name exceeds this limit, the name gets shortened when you add this datastore to vCenter Server.
  After you define a volume label, you can use it whenever you specify the VMFS datastore for the `vmkfstools` command. The volume label appears in listings generated for the `ls -l` command and as a symbolic link to the VMFS volume under the `/vmfs/volumes` directory.
  To change the VMFS volume label, use the `ln -sf` command. Use the following as an example:
  ```
  ln -sf /vmfs/volumes/UUID /vmfs/volumes/datastore
  ```
  `datastore` is the new volume label to use for the *`UUID`* VMFS.
  Note: If your host is registered with vCenter Server, any changes you make to the VMFS volume label get overwritten by vCenter Server. This operation guarantees that the VMFS label is consistent across all vCenter Server hosts.
- `-Y|--unmapGranularity #[bBsSkKmMgGtT]` - This suboption applies to VMFS6 only. Define granularity for the unmap operation. The default granularity is 1 MB. As with the block size, enter the unit type.
- `-O|--unmapPriority <none|low|medium|high>` - This suboption applies to VMFS6 only. Define the priority for the unmap operation.

Example for Creating a VMFS File System

This example illustrates creating a VMFS6 datastore named my_vmfs on the `naa.`*`ID`*`:1` partition.

```
~ vmkfstools -C vmfs6 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

Adding an Extent to a VMFS Datastore

Use the `vmkfstools` command to add an extent to a VMFS datastore.

When you add an extent, you span the VMFS datastore from the head partition across the partition specified by *`span_partition`*.

```
-Z|--spanfs span_partitionhead_partition
```

You must specify the full path name for the head and span partitions, for example `/vmfs/devices/disks/`*`disk_ID:1`* . Each time you use this option, you add an extent to the VMFS datastore, so that the datastore spans multiple partitions.

CAUTION: When you run this option, you lose all data that previously existed on the SCSI device you specified in *`span_partition`*.

Example for Extending a VMFS Datastore

In this example, you extend the existing head partition of the VMFS datastore over a new partition.

```
~ vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

The extended datastore spans two partitions, `naa.`*`disk_ID_1`*`:1` and `naa.`*`disk_ID_2`*`:1` . In this example, `naa.`*`disk_ID_1`*`:1` is the name of the head partition.

Expanding a VMFS Datastore

Instead of adding an extent to a VMFS datastore, you can increase the size of an existing datastore. Use the `vmkfstools -G` command.

You might increase the datastore size after the underlying storage had its capacity increased.

The command uses the following option:

```
-G|--growfs devicedevice
```

This option expands the VMFS datastore or its specific extent. For example,

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

Virtual Disk Options

Virtual disk options allow you to set up, migrate, and manage virtual disks stored on your datastores. You can also perform most of these tasks through the vSphere Client.

Supported Disk Formats

When you create or clone a virtual disk, you can use the `-d|--diskformat` suboption to specify the format for the disk.

Choose from the following formats:

- `zeroedthick` (default) – Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand on first write from the virtual machine. The virtual machine does not read stale data from disk.
- `eagerzeroedthick` – Space required for the virtual disk is allocated at creation time. In contrast to `zeroedthick` format, the data remaining on the physical device is zeroed out during creation. It might take much longer to create disks in this format than to create other types of disks.
- `thin` – Thin-provisioned virtual disk. Unlike with the `thick` format, space required for the virtual disk is not allocated during creation, but is supplied, zeroed out, on demand.
- `rdm:` *`device`* – Virtual compatibility mode raw disk mapping.
- `rdmp:` *`device`* – Physical compatibility mode (pass-through) raw disk mapping.
- `2gbsparse` – A sparse disk with the maximum extent size of 2 GB. You can use disks in this format with hosted VMware products, such as VMware Fusion. However, you cannot power on the sparse disk on an ESXi host unless you first re-import the disk with `vmkfstools` in a compatible format, such as `thick` or `thin` .

Disk Formats on NFS Datastores

The only disk formats you can use for NFS are `thin` , `thick` , `zeroedthick` , and `2gbsparse` .

`Thick` , `zeroedthick` , and `thin` formats usually behave the same because the NFS server and not the ESXi host determines the allocation policy. The default allocation policy on most NFS servers is `thin` . However, on NFS servers that support Storage APIs - Array Integration, you can create virtual disks in `zeroedthick` format. The reserve space operation enables NFS servers to allocate and guarantee space.

For more information on array integration APIs, see Storage Hardware Acceleration.

Creating a Virtual Disk

Use the `vmkfstools` command to create a virtual disk.

```
-c|--createvirtualdisk size[bB|sS|kK|mM|gG]
      -d|--diskformat [thin|zeroedthick|eagerzeroedthick]
```

```
-W|--objecttype [file|vsan|vvol]
--policyFile fileName
```

This option creates a virtual disk at the specified path on a datastore. Specify the size of the virtual disk. When you enter the value for *size*, you can indicate the unit type by adding a suffix of `k` (kilobytes), `m` (megabytes), or `g` (gigabytes). The unit type is not case-sensitive. `vmkfstools` interprets either `k` or `K` to mean kilobytes. If you do not specify a unit type, `vmkfstools` defaults to bytes.

You can specify the following suboptions with the `-c` option.

- `-d|--diskformat` specifies disk formats.
- `-W|--objecttype` specifies whether the virtual disk is a file on a VMFS or NFS datastore, or an object on a vSAN or Virtual Volumes datastore.
- `--policyFile` *fileName* specifies VM storage policy for the disk.

Example for Creating a Virtual Disk

This example shows how to create a two-gigabyte virtual disk file named `disk.vmdk`. You create the disk on the VMFS datastore named `myVMFS` . The disk file represents an empty virtual disk that virtual machines can access.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/disk.vmdk
```

Initializing a Virtual Disk

Use the `vmkfstools` command to initialize a virtual disk.

```
-w|--writezeros
```

This option cleans the virtual disk by writing zeros over all its data. Depending on the size of your virtual disk and the I/O bandwidth to the device hosting the virtual disk, completing this command might take a long time.

CAUTION: When you use this command, you lose any existing data on the virtual disk.

Inflating a Thin Virtual Disk

Use the `vmkfstools` command to inflate a thin virtual disk.

```
-j|--inflatedisk
```

This option converts a `thin` virtual disk to `eagerzeroedthick` , preserving all existing data. The option allocates and zeroes out any blocks that are not already allocated.

Converting a Zeroedthick Virtual Disk to an Eagerzeroedthick Disk

Use the `vmkfstools` command to convert any zeroedthick virtual disk to an eagerzeroedthick disk.

```
-k|--eagerzero
```

While performing the conversion, this option preserves any data on the virtual disk.

Follow this example:

```
vmkfstools --eagerzero /vmfs/volumes/myVMFS/VMName/disk.vmdk
```

Removing Zeroed Blocks

Use the `vmkfstools` command to remove zeroed blocks.

```
-K|--punchzero
```

This option deallocates all zeroed out blocks and leaves only those blocks that were allocated previously and contain valid data. The resulting virtual disk is in thin format.

Deleting a Virtual Disk

Use the vmkfstools command to delete a virtual disk file at the specified path on the VMFS volume.

Use the following option:

```
-U|--deletevirtualdisk
```

Renaming a Virtual Disk

Use the vmkfstools command to rename a virtual disk file at the specified path on the VMFS volume.

You must specify the original filename or file path *`oldName`* and the new filename or file path *`newName`*.

```
-E|--renamevirtualdisk oldNamenewName
```

Cloning or Converting a Virtual Disk or RDM

Use the vmkfstools command to create a copy of a virtual disk or raw disk you specify.

A non-root user cannot clone a virtual disk or an RDM. You must specify the original filename or file path *`oldName`* and the new filename or file path *`newName`*.

```
-i|--clonevirtualdisk oldNamenewName
     -d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device|2gbsparse]
     -W|--objecttype [file|vsan|vvol]
     --policyFile fileName
     -N|--avoidnativeclone
```

Use the following suboptions to change corresponding parameters for the copy you create.

- `-d|--diskformat` specifies disk formats.
- `-W|--objecttype` specifies whether the virtual disk is a file on a VMFS or NFS datastore, or an object on a vSAN or Virtual Volumes datastore.
- `--policyFile` *`fileName`* specifies VM storage policy for the disk.

By default, ESXi uses its native methods to perform the cloning operations. If your array supports the cloning technologies, you can off-load the operations to the array. To avoid the ESXi native cloning, specify the `-N|--avoidnativeclone` option.

Example for Cloning or Converting a Virtual Disk

This example illustrates cloning the contents of a primary virtual disk from the `templates` repository to a virtual disk file named `myOS.vmdk` on the `myVMFS` file system.

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-primary.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

You can configure a virtual machine to use this virtual disk by adding lines to the virtual machine configuration file, as in the following example:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

If you want to convert the format of the disk, use the `-d|--diskformat` suboption.

This suboption is useful when you import virtual disks in a format not compatible with ESXi, for example 2gbsparse format. After you convert the disk, you can attach this disk to a new virtual machine you create in ESXi.

For example:

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-primary.vmdk /vmfs/volumes/myVMFS/myOS.vmdk  -d
 thin
```

Extending a Virtual Disk

After you create a virtual machine, you can use the vmkfstools command to extend the size of a disk allocated to the virtual machine.

```
-X|--extendvirtualdisk newSize[bBsSkKmMgGtT]
```

Specify the `newSize` parameter adding an appropriate unit suffix. The unit type is not case-sensitive. `vmkfstools` interprets either `k` or `K` to mean kilobytes. If you do not specify the unit type, `vmkfstools` defaults to kilobytes.

The `newSize` parameter defines the entire new size, not just the increment you add to the disk.

For example, to extend a 4-g virtual disk by 1 g, enter: `vmkfstools -X 5g`*`disk name`*.

You can extend the virtual disk to the eagerzeroedthick format by using the `-d eagerzeroedthick` option.

When you use the `-X` option, the following considerations apply:

- Do not extend the base disk of a virtual machine that has snapshots associated with it. If you do, you can no longer commit the snapshot or revert the base disk to its original size.
- After you extend the disk, you might need to update the file system on the disk. As a result, the guest operating system recognizes the new size of the disk and can use it.

Upgrading Virtual Disks

This option converts the specified virtual disk file from ESX Server 2 formats to the ESXi format.

Use this option to convert virtual disks of type LEGACYSPARSE, LEGACYPLAIN, LEGACYVMFS, LEGACYVMFS_SPARSE, and LEGACYVMFS_RDM.

```
-M|--migratevirtualdisk
```

Creating a Virtual Compatibility Mode Raw Device Mapping

Use the vmkfstools command to create a Raw Device Mapping (RDM) file on a VMFS volume and map a raw LUN to this file. After this mapping is established, you can access the LUN as you would a normal VMFS virtual disk. The file length of the mapping is the same as the size of the raw LUN it points to.

```
-r|--createrdm device
```

When specifying the *`device`* parameter, use the following format:

```
/vmfs/devices/disks/disk_ID:P
```

Example for Creating a Virtual Compatibility Mode RDM

In this example, you create an RDM file named *my_rdm.vmdk* and map the *disk_ID* raw disk to that file.

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

You can configure a virtual machine to use the `my_rdm.vmdk` mapping file by adding the following lines to the virtual machine configuration file:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Creating a Physical Compatibility Mode Raw Device Mapping

Use the vmkfstools command to map a pass-through raw device to a file on a VMFS volume. With the mapping, a virtual machine can bypass ESXi SCSI command filtering when accessing its virtual disk. This type of mapping is useful when the virtual machine must send proprietary SCSI commands, for example, when SAN-aware software runs on the virtual machine.

```
-z|--createrdmpassthru deviceexample.vmdk
```

After you establish this type of mapping, you can use it to access the raw disk as you access any other VMFS virtual disk.

When specifying the *device* path, use the following format:

```
/vmfs/devices/disks/device_ID
```

For the .vmdk name, use this format. Make sure to create the datastore before using the command.

```
/vmfs/volumes/datastore_name/example.vmdk
```

For example,

```
vmkfstools -z /vmfs/devices/disks/naa.600a0000000000000... /vmfs/volumes/datastore1/mydisk.vmdk
```

Listing Attributes of an RDM

Use the vmkfstools command to list the attributes of a raw disk mapping. The attributes help you identify the storage device to which your RDM files maps.

```
-q|--queryrdm my_rdm.vmdk
```

This option prints the name of the raw disk RDM. The option also prints other identification information, like the disk ID, for the raw disk.

Example of Listing RDM Attributes

```
# vmkfstools -q /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk

Disk /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk is a Passthrough Raw Device Mapping

Maps to: vml.0200000000600507680190020770000000000000005323134352020
```

Displaying Virtual Disk Geometry

Use the vmkfstools command to get information about the geometry of a virtual disk.

```
-g|--geometry
```

The output is in the form: `Geometry information C/H/S` , where `C` represents the number of cylinders, `H` represents the number of heads, and `S` represents the number of sectors.

Note: When you import virtual disks from hosted VMware products to the ESXi host, you might see a disk geometry mismatch error message. A disk geometry mismatch might also trigger problems when you load a guest operating system or run a newly created virtual machine.

Checking and Repairing Virtual Disks

Use the vmkfstools command to check or repair a virtual disk if it gets corrupted.

```
-x|--fix [check|repair]
```

For example,

```
vmkfstools -x check /vmfs/volumes/my_datastore/my_disk.vmdk
```

Checking Disk Chain for Consistency

Use the vmkfstools command to check the entire snapshot chain. You can determine if any of the links in the chain are corrupted or any invalid parent-child relationships exist.

```
-e|--chainConsistent
```

Storage Device Options

You can use the device options of the vmkfstools command to perform administrative task for physical storage devices.

Managing SCSI Reservations of LUNs

Use the vmkfstools command to reserve a SCSI LUN for exclusive use by the ESXi host. You can also release a reservation so that other hosts can access the LUN, and reset a reservation, forcing all reservations from the target to be released.

```
-L|--lock [reserve|release|lunreset|targetreset|busreset|readkeys|readresv] device
```

CAUTION: Using the `-L` option can interrupt the operations of other servers on a SAN. Use the `-L` option only when troubleshooting clustering setups.

Unless advised by VMware, never use this option on a LUN hosting a VMFS volume.

You can specify the `-L` option in several ways:

- `-L reserve` – Reserves the specified LUN. After the reservation, only the server that reserved that LUN can access it. If other servers attempt to access that LUN, a reservation error appears.
- `-L release` – Releases the reservation on the specified LUN. Other servers can access the LUN again.
- `-L lunreset` – Resets the specified LUN by clearing any reservation on the LUN and making the LUN available to all servers again. The reset does not affect any of the other LUNs on the device. If another LUN on the device is reserved, it remains reserved.
- `-L targetreset` – Resets the entire target. The reset clears any reservations on all the LUNs associated with that target and makes the LUNs available to all servers again.
- `-L busreset` – Resets all accessible targets on the bus. The reset clears any reservation on all the LUNs accessible through the bus and makes them available to all servers again.
- `-L readkeys` – Reads the reservation keys registered with a LUN. Applies to SCSI-III persistent group reservation functionality.
- `-L readresv` – Reads the reservation state on a LUN. Applies to SCSI-III persistent group reservation functionality.

When entering the *device* parameter, use the following format:

```
/vmfs/devices/disks/disk_ID:P
```

Breaking Device Locks

Use the vmkfstools command to break the device lock on a particular partition.

```
-B|--breaklock device
```

When entering the *device* parameter, use the following format:

```
/vmfs/devices/disks/disk_ID:P
```

You can use this command when a host fails in the middle of a datastore operation, such as expand the datastore, add an extent, or resignature. When you run this command, make sure that no other host is holding the lock.

vSphere Security

vSphere Security provides information about securing your vSphere® environment for VMware® vCenter® Server and VMware ESXi.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

To help you protect your vSphere environment, this documentation describes available security features and the measures that you can take to safeguard your environment from attack.

Table 230: *vSphere Security* Highlights

Topics	Content Highlights
Permissions and User Management	• Permissions model (roles, groups, objects). • Creating custom roles. • Setting permissions. • Managing global permissions.
Host Security Features	• Lockdown mode and other security profile features. • Host smart card authentication. • vSphere Authentication Proxy. • UEFI Secure Boot. • Trusted Platform Module (TPM). • VMware®vSphere Trust Authority™. • Secure ESXi Configuration and configuration sealing
Virtual Machine Encryption	• VMware vSphere® Native Key Provider™. • How does VM encryption work? • KMS setup. • Encrypting and decrypting VMs. • Troubleshooting and best practices.
Guest OS Security	• Virtual Trusted Platform Module (vTPM). • Virtualization Based Security (VBS).
Managing TLS Protocol Configuration	Changing TLS protocol configuration using a command-line utility.
Security Best Practices and Hardening	Best practices and advice from VMware security experts. • vCenter Server security • Host security • Virtual machine security • Networking security
vSphere Privileges	Complete listing of all vSphere privileges supported in this release.

Related Documentation

A companion document, *vSphere Authentication*, explains how you can use authentication services, for example, to manage authentication with vCenter Single Sign-On and to manage certificates in your vSphere environment.

In addition to these documents, VMware publishes the *vSphere Security Configuration Guide* (formerly known as the *Hardening Guide*) for each release of vSphere, accessible at https://core.vmware.com/security. The *vSphere Security Configuration Guide* contains guidelines on security settings that can or should be set by the customer, and security settings delivered by VMware that should be audited by the customer to ensure that they are still set to default.

What Happened to the Platform Services Controller

Beginning in vSphere 7.0, deploying a new vCenter Server or upgrading to vCenter Server 7.0 requires the use of the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server appliance, see the *vSphere Upgrade* documentation.

Intended Audience

This information is for experienced system administrators who are familiar with virtual machine technology and data center operations.

Certifications

VMware publishes a public list of VMware products that have completed Common Criteria certifications. To check if a particular VMware product version has been certified, see the Common Criteria Evaluation and Validation webpage at https://www.vmware.com/security/certifications/common-criteria.html.

Updated Information

This *vSphere Security* document is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Security* documentation.

Revision	Description
29 AUG 2024	• Minor update to Create a Virtual Machine with a Virtual Trusted Platform Module. • Updated video links.
07 AUG 2024	• Minor update to Create a Virtual Machine with a Virtual Trusted Platform Module. • Minor update to Defined Privileges. • Minor update to Profile-driven Storage Privileges. • Removed references to the `vifs` command. See the VMware knowledge base article at https://kb.vmware.com/kb/78473.
25 JUL 2024	• Minor update to Managing ESXi Audit Records.
24 JUL 2024	• Clarified how audit records are stored and transmitted in Managing ESXi Audit Records.
12 JUN 2024	• Minor update to Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration. • Minor update to Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration.
04 JUN 2024	• Minor update to vSphere Encryption Keys and Key Providers. • Minor update to Create a Virtual Machine with a Virtual Trusted Platform Module.
08 MAR 2024	• Added new topic, Delete a Standard Key Provider.

Revision	Description
01 FEB 2024	• Minor update to Activate or Deactivate UEFI Secure Boot for a Virtual Machine.
22 JAN 2024	• Minor update to ESXi Certificate Default Settings.
10 JAN 2024	• Minor update to Set Up vSphere Authentication Proxy to Use Custom Certificates. • Minor update to Decrypt an Encrypted Virtual Machine or Virtual Disk.
11 DEC 2023	• Minor update to Unlock Locked Virtual Machines. • Minor update to Scan vCenter Server for Enabled TLS Protocols. • Minor update to vSphere with Tanzu Privileges.
17 NOV 2023	• Updated the vSphere Inventory Hierarchy figure in Hierarchical Inheritance of Permissions. • Minor update to ESXi Pass Phrase. • Minor update to ESXi Certificate Default Settings. • Minor update to Add Users to the DCUI.Access Advanced Option. • Minor update to Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration. • Minor update to Restore a vSphere Native Key Provider Using the vSphere Client. • Updated Create a Virtual Machine with a Virtual Trusted Platform Module and Enable Virtual Trusted Platform Module for an Existing Virtual Machine to state that the **Cryptographic operations** > **Direct Access** privilege is required to open a console session. • Minor update to Enable or Disable TLS Versions on vCenter Server Systems. • Minor update to Sessions Privileges.
27 APR 2023	• Minor update to Replace a Default Certificate Using HTTPS PUT. • Minor update to Managing ESXi Audit Records.
21 MAR 2023	• Minor update to Virtual Disk Encryption. • Minor update to Encrypt an Existing Virtual Machine or Virtual Disk. • Minor update to vSphere Native Key Provider Overview. • Minor update to Back up a vSphere Native Key Provider.
07 MAR 2023	• Minor update to Troubleshooting and Recovering the Secure ESXi Configuration. • Minor update to Recover the Secure ESXi Configuration.
15 FEB 2023	• Minor update to Recover the Secure ESXi Configuration. • Minor update to Virtual Machine Encryption Interoperability.
31 JAN 2023	• Updated How vSphere Virtual Machine Encryption Protects Your Environment and Prerequisites and Required Privileges for Encryption Tasks to state that ESXi Shell users also have cryptographic operation privileges. • Minor update to Enable Virtualization-based Security on a Virtual Machine and Enable Virtualization-based Security on an Existing Virtual Machine.

Revision	Description
23 JAN 2023	• Minor update to vSphere Native Key Provider Overview. • Updated Enable Virtual Trusted Platform Module for an Existing Virtual Machine to state that the **Virtual machine** > **Configuration** > **Add or remove device** privilege is required.
23 DEC 2022	• Minor update to Collect a vm-support Package for an ESXi Host That Uses Encryption. • Minor update to Enable and Disable Key Persistence on an ESXi Host. • Minor update to Remove Virtual Trusted Platform Module from a Virtual Machine.
23 NOV 2022	• Minor update to vCenter Server System Roles. • Updated Key Persistence Overview and Enable and Disable Key Persistence on an ESXi Host with additional information about vSphere Native Key Provider. • Minor update to Secure VLANs.
13 OCT 2022	• Minor update to Managing ESXi Audit Records. • Fixed typo in Update a vSphere Native Key Provider. • Minor updates to Virtualization-based Security Best Practices, Enable Virtualization-based Security on a Virtual Machine, and Enable Virtualization-based Security on an Existing Virtual Machine. • Removed references to the `vifs` command. See the VMware knowledge base article at https://kb.vmware.com/kb/78473.
22 AUG 2022	• Minor update to Renew or Refresh ESXi Certificates. • Minor update to Delete a vSphere Native Key Provider. • Fixed the example in Create the Key Provider on the Trust Authority Cluster. • Rewrote Disable Host Encryption Mode Using the API to use the vCenter Server Managed Object Browser (MOB). • Minor update to multiple VMware vSphere Lifecycle Manager privileges topics.
28 JUL 2022	• Minor update to Requirements for ESXi Certificate Signing Requests. • Minor update to Virtual Trusted Platform Module Overview. • Minor update to MAC Address Changes. • Updated multiple topics to note that you should assign privileges that use VMware vSphere Lifecycle Manager APIs that accept URLs only to administrators or trusted users.
12 JUL 2022	• Minor update to Change User Validation Settings. • Minor update to Renew or Refresh ESXi Certificates. • Minor update to Activate Fault Tolerance Encryption. • Fixed problem with the formatting of an ESXCLI command in Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration. • Minor update to Disable Unused Display Features. • Removed parameters that are now set to TRUE from Disable Unexposed Features. • Corrected the steps in Create an Encryption Storage Policy.

Revision	Description
15 JUN 2022	• Added information about vCenter Server and encrypted communication to Securing vCenter Server Systems and Associated Services. • Added information about assigning permissions on vSphere Distributed Switches to Hierarchical Inheritance of Permissions. • Minor update to UEFI Secure Boot for ESXi Hosts. • Added information about encryption considerations to Virtual Machine Encryption Best Practices. • Minor update to vSphere Native Key Provider Overview. • Added information about `HostCryptoState` to Disable Host Encryption Mode Using the API. • Added a required privilege, **Cryptographic operations** > **Migrate**, to Create a Virtual Machine with a Virtual Trusted Platform Module and Enable Virtual Trusted Platform Module for an Existing Virtual Machine. This privilege enables a virtual machine to be powered on when DRS starts it on another host. • Minor update to Connecting to the Virtual Machine Console Through a Firewall. • Minor update to Enable or Disable TLS Versions on ESXi Hosts. • Added information about setting permissions to Content Library Privileges. • Fixed typo in vSphere Tagging Privileges.
29 APR 2022	• In Managing ESXi Audit Records, the `viewAudit` program replaces the `auditLogReader` program as of vSphere 7.0 Update 3d. • Minor updates to Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration and Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration. • Minor updates to How vSphere Virtual Machine Encryption Protects Your Environment. • Updated information about vSphere Native Key Provider and key persistence in Key Persistence Overview, Back up a vSphere Native Key Provider, and Enable and Disable Key Persistence on an ESXi Host. • Minor update to vSphere Native Key Provider Overview. • Fixed commands in Update a vSphere Native Key Provider. • Minor update to Connecting ESXi Hosts Through Firewalls. • Minor update to Storage Views Privileges.
10 MAR 2022	• Minor update to Host Upgrades and Certificates. • Fixed incorrect commands in step 4 in Use Custom Certificates with Auto Deploy. • Updated the prerequisites in Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine with the vSphere Client, Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine, Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine with the vSphere Client, and Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine. • Minor update to Virtual Machine Encryption Interoperability.

Revision	Description
	• Updated vSphere Native Key Provider Overview to state that the vSphere Native Key Provider does not require a TPM 2.0. • In Configure the Trusted Key Provider for Trusted Hosts Using the vSphere Client and Configure the Trusted Key Provider for Trusted Hosts Using the Command Line, clarified that when you add a vSphere Trust Authority key provider, it takes some time for the key provider to become available for use. • Added required privileges to Create a Virtual Machine with a Virtual Trusted Platform Module, Enable Virtual Trusted Platform Module for an Existing Virtual Machine, and Remove Virtual Trusted Platform Module from a Virtual Machine.
19 JAN 2022	• Minor update to Understanding Authorization in vSphere. • Minor update to Restore ESXi Certificate and Key Files. • For a standalone ESXi host, clarified that you must run the `reconfigureEsx ESXiHost` command from a vCenter Server system in Enable or Disable TLS Versions on ESXi Hosts. • Updated Considerations When Using FIPS with information about the vCenter Server file-based backup and restore.
21 DEC 2021	• Minor update to TPM Sealing Policies Overview. • Minor update to Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration. • Minor update to Resolve ESXi Host Encryption Mode Issues. • Minor update to Encrypted vSphere vMotion.
07 DEC 2021	• Minor update to Comparison of vSphere Key Providers. • Added new topic, Import a vSphere Native Key Provider in an Enhanced Linked Mode Configuration. • Minor update to vSphere Trust Authority Best Practices, Caveats, and Interoperability. • Added new topic, Rekey an Encrypted Virtual Machine Using the vSphere Client. • Updated Content Library Privileges with new privileges. • Updated vSphere with Tanzu Privileges with new privileges.
03 NOV 2021	• Minor update to Securing the Virtual Networking Layer. • Minor update to Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration. • Updated View Certificate Expiration Information for Multiple ESXi Hosts, Identify Virtual Trusted Platform Module Enabled Virtual Machines, View Virtual Trusted Platform Module Device Certificates, and Identify VBS-Enabled Virtual Machines to reflect a minor UI change with how to show and hide columns. • Updated Manage ESXi Firewall Settings and Add Allowed IP Addresses for an ESXi Host to reflect minor UI changes. • Added encryption-related information to Virtual Machine Encryption Interoperability. • Updated MAC Address Changes and Forged Transmits to reflect the change in the default for both options from Accept to Reject. • Corrected a privilege in Virtual Machine Provisioning Privileges. • Minor update to Single Sign-On Audit Events.
05 OCT 2021	Initial release.

Security in the vSphere Environment

The components of a vSphere environment are secured out of the box by several features such as authentication, authorization, a firewall on each ESXi host, and so on. You can modify the default setup in many ways. For example, you can set permissions on vCenter objects, open firewall ports, or change the default certificates. You can take security measures for different objects in the vCenter object hierarchy, for example, vCenter Server systems, ESXi hosts, virtual machines, and network and storage objects.

A high-level overview of different areas of vSphere that require attention helps you plan your security strategy. You also benefit from other vSphere Security resources on the VMware Web site.

Securing the ESXi Hypervisor

The ESXi hypervisor is secured out of the box. You can further protect ESXi hosts by using lockdown mode and other built-in features. For consistency, you can set up a reference host and keep all hosts in sync with the host profile of the reference host. You can also protect your environment by performing scripted management, which ensures that changes apply to all hosts.

You can enhance protection of ESXi hosts that are managed by vCenter Server with the following actions. See the *Security of the VMware vSphere Hypervisor* white paper for background and details.

Limit ESXi access	By default, the ESXi Shell and SSH services are not running and only the root user can log in to the Direct Console User Interface (DCUI). If you decide to enable ESXi or SSH access, you can set timeouts to limit the risk of unauthorized access. Users who can access the ESXi host must have permissions to manage the host. You set permissions on the host object from the vCenter Server system that manages the host.
Use named users and least privilege	By default, the root user can perform many tasks. Do not allow administrators to log in to the ESXi host using the root user account. Instead, create named administrator users from vCenter Server and assign those users the Administrator role. You can also assign those users a custom role. See Create a vCenter Server Custom Role. If you manage users directly on the host, role management options are limited. See the *vSphere Single Host Management - VMware Host Client* documentation.
Minimize the number of open ESXi firewall ports	By default, firewall ports on your ESXi host are opened only when you start a corresponding service. You can use the vSphere Client or ESXCLI or PowerCLI commands to check and manage firewall port status. See ESXi Firewall Configuration.
Automate ESXi host management	Because it is often important that different hosts in the same data center are in sync, use scripted installation or vSphere Auto Deploy to provision hosts. You can manage the hosts using scripts. Host profiles are an alternative to scripted management. You set up a reference host, export the host profile, and apply the host profile to all hosts. You can apply the host profile directly or as part of provisioning with Auto Deploy. See Use Scripts to Manage Host Configuration Settings and see the *vCenter Server Installation and Setup* documentation for information about vSphere Auto Deploy.
Take advantage of lockdown mode	In lockdown mode, ESXi hosts can be accessed only through vCenter Server by default. You can select strict lockdown mode or normal lockdown mode. You can define Exception Users to allow direct access to service accounts such as backup agents. See Lockdown Mode.

Check VIB package integrity	Each VIB package has an associated acceptance level. You can add a VIB to an ESXi host only if the VIB acceptance level is the same or better than the acceptance level of the host. You cannot add a CommunitySupported or PartnerSupported VIB to a host unless you explicitly change the host's acceptance level. See Manage the Acceptance Levels of Hosts and VIBs.
Manage ESXi certificates	The VMware Certificate Authority (VMCA) provisions each ESXi host with a signed certificate that has VMCA as the root certificate authority by default. If your company policy requires it, you can replace the existing certificates with certificates that are signed by a third-party or an enterprise CA. See Certificate Management for ESXi Hosts.
Consider Smart card authentication	ESXi supports the use of smart card authentication instead of user name and password authentication. For additional security, you can configure smart card authentication. Two-factor authentication is also supported for vCenter Server. You can configure user name and password authentication and smart card authentication at the same time. See Configuring Smart Card Authentication for ESXi.
Consider ESXi account lockout	Account locking is supported for access through SSH and through the vSphere Web Services SDK. By default, a maximum of 10 failed attempts is allowed before the account is locked. The account is unlocked after two minutes by default. **Note:** The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. See ESXi Passwords and Account Lockout.

Security considerations for standalone hosts are similar, though the management tasks might differ. See the *vSphere Single Host Management - VMware Host Client* documentation.

Securing vCenter Server Systems and Associated Services

Your vCenter Server system and associated services are protected by authentication through vCenter Single Sign-On and by authorization through the vCenter Server permissions model. You can modify the default behavior, and you can take steps to limit access to your environment.

As you protect your vSphere environment, consider that all services that are associated with the vCenter Server instances must be protected. In some environments, you might protect several vCenter Server instances.

vCenter and encrypted communication	By default ("out of the box"), all data communication between vCenter Server and other vSphere components is encrypted. In some cases, depending on how you configure your environment, some traffic might be unencrypted. For example, you can configure unencrypted SMTP for email alerts and unencrypted SNMP for monitoring. DNS traffic is also unencrypted. vCenter Server listens on port 80 (TCP) and port 443 (TCP). Port 443 (TCP) is the industry-standard HTTPS (secure HTTP) port and uses TLS 1.2 encryption for protection. Port 80 (TCP) is the industry-standard HTTP port and does not use encryption. The purpose of port 80 is to redirect requests from port 80 to port 443, where they are secure.
Harden all vCenter host machines	The first step in protecting your vCenter environment is hardening each machine on which vCenter Server or an associated service runs. Similar considerations apply to a physical machine or a virtual machine. Always install the latest security patches for your operating system and follow industry standard best practices to protect the host machine.

Learn about the vCenter certificate model	By default, the VMware Certificate Authority provisions each ESXi host and each machine in the environment with a certificate signed by VMCA. If your company policy requires it, you can change the default behavior. See the *vSphere Authentication* documentation for details. For additional protection, explicitly remove expired or revoked certificates and failed installations.
Configure vCenter Single Sign-On	vCenter Server and associated services are protected by the vCenter Single Sign-On authentication framework. When you first install the software, you specify a password for the administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default. Only that domain is initially available as an identity source. You can add an external identity provider, such as Microsoft Active Directory Federation Services (AD FS), for federated authentication. You can add other identity sources, either Active Directory or LDAP, and set a default identity source. Users who can authenticate to one of those identity sources can view objects and perform tasks if they are authorized to do so. See the *vSphere Authentication* documentation for details.
Assign roles to named users or groups	For better logging, associate each permission that you give on an object with a named user or group and a predefined role or custom role. The vSphere permissions model allows great flexibility through multiple ways of authorizing users or groups. See Understanding Authorization in vSphere and Required vCenter Server Privileges for Common Tasks. Restrict administrator privileges and the use of the administrator role. If possible, do not use the anonymous Administrator user.
Set up PTP or NTP	Set up PTP or NTP for each node in your environment. The certificate infrastructure requires an accurate time stamp and does not work correctly if the nodes are out of sync. See Synchronizing Clocks on the vSphere Network.

Securing Virtual Machines

To secure your virtual machines, keep the guest operating systems patched and protect your environment just as you protect your physical machine. Consider disabling unnecessary functionality, minimize the use of the virtual machine console, and follow other best practices.

Protect the guest operating system	To protect your guest operating system, make sure that it uses the most recent patches and, if appropriate, anti-spyware and anti-malware applications. See the documentation from your guest operating system vendor and, potentially, other information available in books or on the Internet for that operating system.
Disable unnecessary functionality	Check that unnecessary functionality is disabled to minimize potential points of attack. Many of the features that are used infrequently are disabled by default. Remove unnecessary hardware and disable certain features such as host-guest filesystem (HGFS) or copy and paste between the virtual machine and a remote console. See Disable Unnecessary Functions Inside Virtual Machines.
Use templates and scripted management	Virtual machine templates enable you to set up the operating system so that it meets your requirements, and to create other VMs with the same settings. If you want to change virtual machine settings after initial deployment, consider using scripts, for example, PowerCLI. This documentation explains how to perform tasks using the GUI. Consider using scripts instead of the GUI to keep your

	environment consistent. In large environments, you can group virtual machines into folders to optimize scripting. For information on templates, see Use Templates to Deploy Virtual Machines and the *vSphere Virtual Machine Administration* documentation. For information on PowerCLI, see the VMware PowerCLI documentation.
Minimize use of the virtual machine console	The virtual machine console provides the same function for a virtual machine that a monitor on a physical server provides. Users with access to a virtual machine console have access to virtual machine power management and to removable device connectivity controls. As a result, virtual machine console access might allow a malicious attack on a virtual machine.
Consider UEFI secure boot	You can configure your virtual machine to use UEFI boot. If the operating system supports secure UEFI boot, you can select that option for your VMs for additional security. See Activate or Deactivate UEFI Secure Boot for a Virtual Machine.
Consider Carbon Black Cloud Workload	You can install and use Carbon Black Cloud Workload to identify risk, prevent attacks, and detect unusual activities. With the AppDefense functionality built in to the Carbon Black Cloud platform, Carbon Black Cloud Workload is the successor product for AppDefense.

Securing the Virtual Networking Layer

The virtual networking layer includes virtual network adapters, virtual switches, distributed virtual switches, and ports and port groups. ESXi relies on the virtual networking layer to support communications between VMs and their users. In addition, ESXi uses the virtual networking layer to communicate with iSCSI SANs, NAS storage, and so on.

vSphere includes the full array of features necessary for a secure networking infrastructure. You can secure each element of the infrastructure, such as virtual switches, distributed virtual switches, and virtual network adapters, separately. In addition, consider the following guidelines, discussed in more detail in Securing vSphere Networking.

Isolate network traffic	Isolation of network traffic is essential to a secure ESXi environment. Different networks require different access and level of isolation. A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from normal traffic. Ensure that the management network is accessible only by system, network, and security administrators. See ESXi Networking Security Recommendations.
Use firewalls to secure virtual network elements	You can open and close firewall ports and secure each element in the virtual network separately. For ESXi hosts, firewall rules associate services with corresponding firewalls and can open and close the firewall according to the status of the service. You can also open ports on vCenter Server instances explicitly. For the list of all supported ports and protocols in VMware products, including vSphere and vSAN, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/. You can search ports by VMware product, create a customized list of ports, and print or save port lists.
Consider network security policies	Network security policies provide protection of traffic against MAC address impersonation and unwanted port scanning. The security policy of a standard or distributed switch is implemented in Layer 2 (Data Link Layer) of the network protocol stack. The three elements of the security policy are promiscuous mode, MAC address changes, and forged transmits.

Secure VM networking	See the *vSphere Networking* documentation for instructions. The methods that you use to secure VM networking depend on several factors, including: • The guest operating system that is installed • Whether the VMs operate in a trusted environment Virtual switches and distributed virtual switches provide significant protection when used with other common security practices, such as installing firewalls. See Securing vSphere Networking.
Consider VLANs to protect your environment	ESXi supports IEEE 802.1q VLANs. VLANs let you segment a physical network. You can use VLANs to further protect the VM network or storage configuration. When you use VLANS, two VMs on the same physical network cannot send packets to or receive packets from each other unless they are on the same VLAN. See Securing Virtual Machines with VLANs.
Secure connections to virtualized storage	A VM stores operating system files, application files, and other data on a virtual disk. Each virtual disk appears to the VM as a SCSI drive that is connected to a SCSI controller. A VM is isolated from storage details and cannot access the information about the LUN where its virtual disk resides. The Virtual Machine File System (VMFS) is a distributed file system and volume manager that presents virtual volumes to the ESXi host. You are responsible for securing the connection to storage. For example, if you are using iSCSI storage, you can set up your environment to use CHAP. If required by company policy, you can set up mutual CHAP. Use the vSphere Client or CLIs to set up CHAP. See Storage Security Best Practices.
Evaluate the use of IPSec	ESXi supports IPSec over IPv6. You cannot use IPSec over IPv4. See Internet Protocol Security.

Passwords in Your vSphere Environment

Password restrictions, password expiration, and account lockout in your vSphere environment depend on the system that the user targets, who the user is, and how policies are set.

ESXi Passwords

ESXi password restrictions are determined by certain requirements. See ESXi Passwords and Account Lockout.

Passwords for vCenter Server and Other vCenter Services

vCenter Single Sign-On manages authentication for all users who log in to vCenter Server and other vCenter services. The password restrictions, password expiration, and account lockout depend on the user's domain and on who the user is.

vCenter Single Sign-On Administrator	The password for the administrator@vsphere.local user, or the administrator@`mydomain` user if you selected a different domain during installation, does not expire and is not subject to the lockout policy. In all other regards, the password must follow the restrictions that are set in the vCenter Single Sign-On password policy. See *vSphere Authentication* for details. If you forget the password for this user, search the VMware Knowledge Base system for information on resetting this

	password. The reset requires additional privileges such as root access to the vCenter Server system.
Other Users of the vCenter Single Sign-On Domain	Passwords for other vsphere.local users, or users of the domain that you specified during installation, must follow the restrictions that are set by the vCenter Single Sign-On password policy and lockout policy. See *vSphere Authentication* for details. These passwords expire after 90 days by default. Administrators can change the expiration as part of the password policy. If you forget your vsphere.local password, an administrator user can reset the password using the `dir-cli` command.
Other Users	Password restrictions, password expiration, and account lockout for all other users are determined by the domain (identity source) to which the user can authenticate. vCenter Single Sign-On supports one default identity source. Users can log in to the corresponding domain with the vSphere Client with their user names. If users want to log in to a non-default domain, they can include the domain name, that is, specify *`user`*@*`domain`* or *`domain`**`user`*. The domain password parameters apply to each domain.

Passwords for vCenter Server Direct Console User Interface Users

The vCenter Server appliance is a preconfigured virtual machine that is optimized for running vCenter Server and the associated services.

When you deploy the vCenter Server, you specify these passwords.

- Password for the root user.
- Password for the administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default.

You can change the root user password and perform other vCenter Server local user management tasks from the vCenter Server Management Interface. See *vCenter Server Configuration*.

Security Best Practices and Resources

If you follow best practices, yourESXi andvCenter Server can be as secure as or even more secure than an environment that does not include virtualization.

This manual includes best practices for the different components of your vSphere infrastructure.

Table 231: Security Best Practices

vSphere component	Resource
ESXi host	Securing ESXi Hosts
vCenter Server system	vCenter Server Security Best Practices
Virtual machine	Virtual Machine Security Best Practices
vSphere Networking	vSphere Networking Security Best Practices

This manual is only one of the sources you must use to ensure a secure environment.

VMware security resources, including security alerts and downloads, are available on the Web.

Table 232: VMware Security Resources on the Web

Topic	Resource
Information onESXi andvCenter Server security and operations, including secure configuration and hypervisor security.	https://core.vmware.com/security
VMware security policy, up-to-date security alerts, security downloads, and focus discussions of security topics.	http://www.vmware.com/go/security
Corporate security response policy	http://www.vmware.com/support/policies/security_response.html VMware is committed to helping you maintain a secure environment. Security issues are corrected in a timely manner. The VMware Security Response Policy states our commitment to resolve possible vulnerabilities in our products.
Third-party software support policy	http://www.vmware.com/support/policies/ VMware supports a variety of storage systems, software agents such as backup agents, system management agents, and so forth. You can find lists of agents, tools, and other software that supportsESXi by searching http://www.vmware.com/vmtn/resources/ forESXi compatibility guides. The industry offers more products and configurations than VMware can test. If VMware does not list a product or configuration in a compatibility guide, Technical Support attempts to help you with any problems, but cannot guarantee that the product or configuration can be used. Always evaluate security risks for unsupported products or configurations carefully.
Compliance and security standards, and partner solutions and in-depth content about virtualization and compliance	https://core.vmware.com/compliance
Information on security certifications and validations such as CCEVS and FIPS for different versions of the components of vSphere.	https://www.vmware.com/support/support-resources/certifications.html
Security configuration guides (formerly known as hardening guides) for different versions of vSphere and other VMware products.	https://core.vmware.com/security
Security of the VMware vSphere Hypervisor white paper	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere Permissions and User Management Tasks

Authentication and authorization govern access.vCenter Single Sign-On supports authentication, which means it determines whether a user can log in to vSphere components at all. Each user must also be authorized to view or manipulate vSphere objects.

vSphere supports several different authorization mechanisms, discussed in Understanding Authorization in vSphere. This section focuses on how thevCenter Server permission model works and how to perform user management tasks.

vCenter Server allows fine-grained control over authorization with permissions and roles. When you assign a permission to an object in thevCenter Server object hierarchy, you specify which user or group has which privileges on that object. To specify the privileges, you use roles, which are sets of privileges.

Initially, only the administrator user for the vCenter Single Sign-On domain is authorized to log in to thevCenter Server system. The default domain is vsphere.local and the default administrator is administrator@vsphere.local. You can change the default domain during installation of vSphere.

The administrator user can proceed as follows:

1. Add an identity source in which users and groups are defined tovCenter Single Sign-On. See the *vSphere Authentication* documentation.
2. Give privileges to a user or group by selecting an object such as a virtual machine or avCenter Server system and assigning a role on that object for the user or group.

Understanding Authorization in vSphere

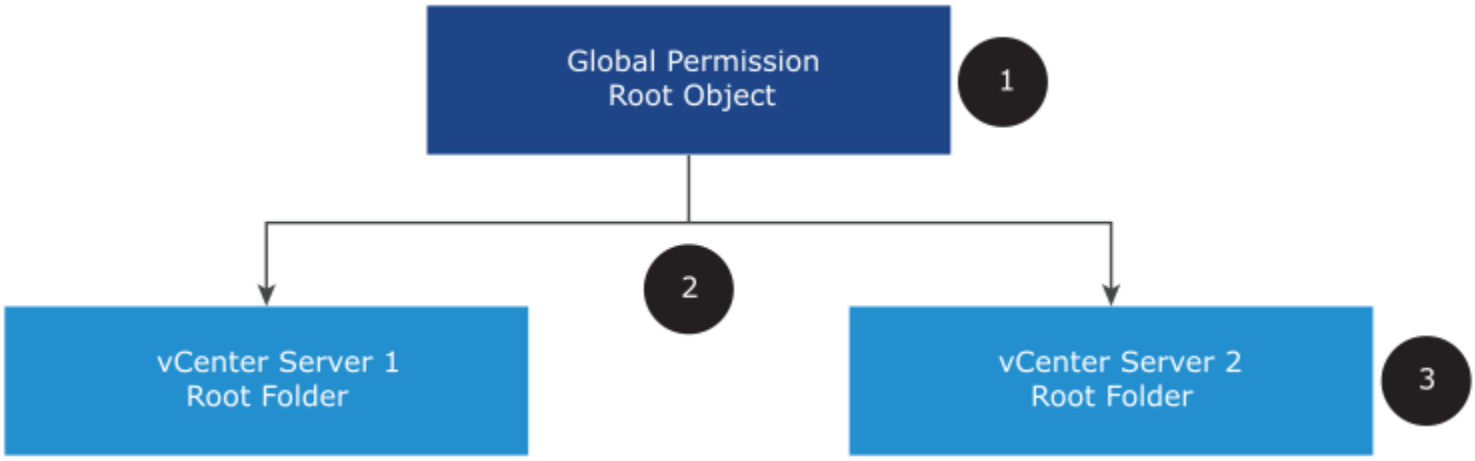
vSphere supports several models for determining whether a user is allowed to perform a task. Group membership in a vCenter Single Sign-On group decides what you are allowed to do. Your role on an object or your global permission determines whether you are allowed to perform other tasks.

How Do Permissions Work in vSphere

vSphere allows privileged users to give other users permissions to perform tasks. You can use global permissions, or you can use localvCenter Server permissions to authorize other users for individualvCenter Server instances.

The following figure illustrates how global and local permissions work.

Figure 82: Global Permissions and Local Permissions



In this figure:

1. You assign a global permission at the root object level with "Propagate to children" selected.
2. vCenter Server propagates the permissions to thevCenter Server 1 andvCenter Server 2 object hierarchies in the environment.
3. A local permission on the root folder onvCenter Server 2 overrides the global permission.

vCenter Server Permissions

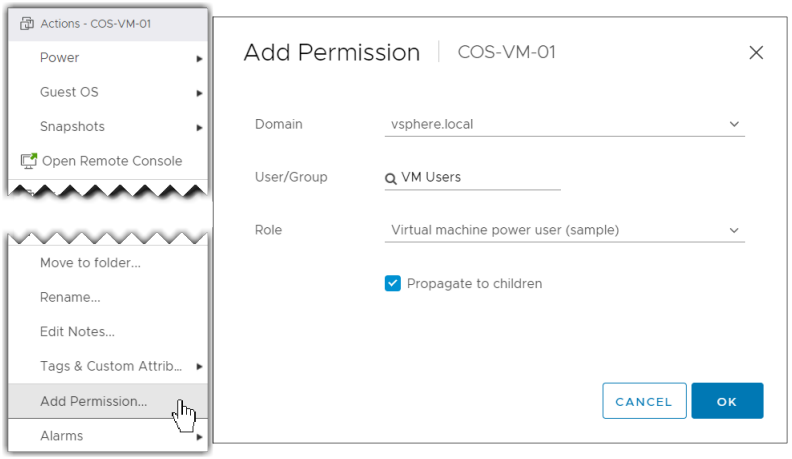
The permission model forvCenter Server systems relies on assigning permissions to objects in the object hierarchy. Users get permissions in the following ways.

- From a specific permission for the user or from the groups that the user is a member of
- From a permission on the object or through the permission inheritance from a parent object

Each permission gives one user or group a set of privileges, that is, a role for a selected object. You can use thevSphere Client to add permissions. For example, you can right-click a virtual machine, select **Add Permission**, and complete the dialog box to

assign a role to a group of users. That role gives those users the corresponding privileges on the virtual machine.

Figure 83: Adding Permissions to a Virtual Machine Using thevSphere Client



Global Permissions

Global permissions give a user or group privileges to view or manage all objects in each of the inventory hierarchies of the solutions in the deployment. That is, global permissions are applied to a global root object that spans solution inventory hierarchies. (Solutions includevCenter Server,VMware vRealize OrchestratorK, and so on.) Global permissions also apply to global objects such as tags and content libraries. For example, consider a deployment that consists of two solutions,vCenter Server andVMware vRealize OrchestratorK. You can use global permissions to assign a role to a group of users that has read-only privileges to all objects in both thevCenter Server andVMware vRealize OrchestratorK object hierarchies.

Group Membership in vCenter Single Sign-On Groups

ESXi Local Host Permissions

If you are managing a standaloneESXi host that is not managed by avCenter Server system, you can assign one of the predefined roles to users. See the *vSphere Single Host Management - VMware Host Client* documentation.

For managed hosts, assign roles to theESXi host object in thevCenter Server inventory.

Understanding the Object-Level Permission Model

You authorize a user or group to perform tasks onvCenter Server objects by using permissions on the object. From a programmatic standpoint, when a user tries to perform an operation, an API method is executed.vCenter Server checks the permissions for that method to see if the user is authorized to perform the operation. For example, when a user tries to add a host, the `AddStandaloneHost_Task` method is invoked. This method requires that the role for the user has the Host.Inventory.AddStandaloneHost privilege. If the check does not find this privilege, the user is denied permission to add the host.

The following concepts are important.

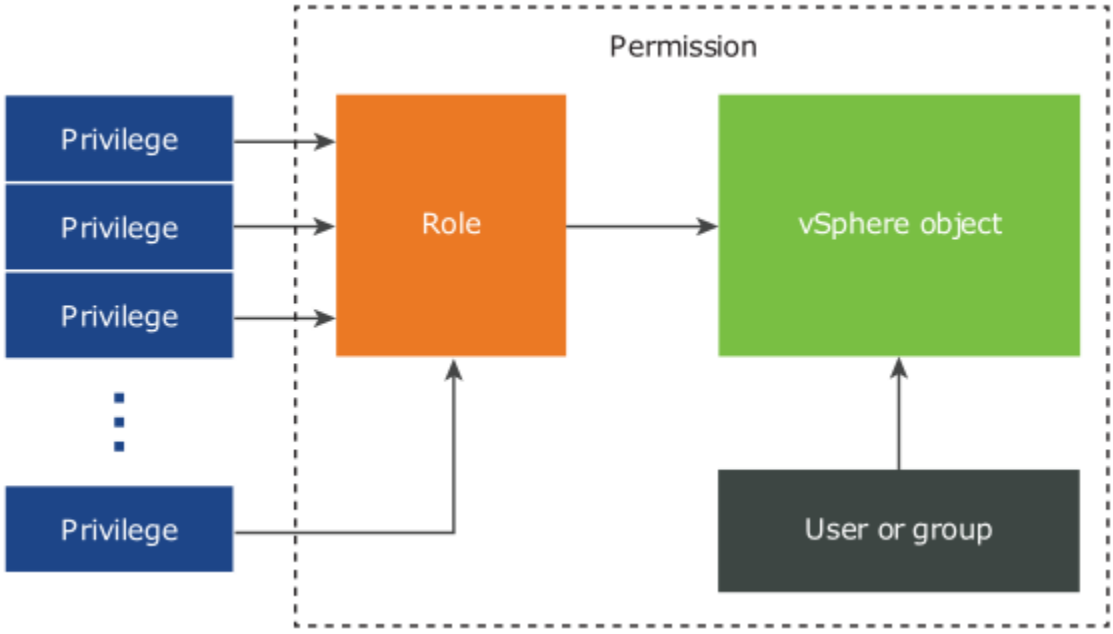
Permissions

Each object in the object hierarchy has associated permissions. Each permission specifies for one group or user which privileges

	that group or user has on the object. Permissions can propagate to child objects.
Users and Groups	On systems, you can assign privileges only to authenticated users or groups of authenticated users. Users are authenticated through. Users and groups must be defined in the identity source that uses to authenticate. Define users and groups using the tools in your identity source, for example, Active Directory.
Privileges	Privileges are fine-grained access controls. You can group those privileges into roles, which you can then map to users or groups.
Roles	Roles are sets of privileges. Roles allow you to assign permissions on an object based on a typical set of tasks that users perform. System roles, such as Administrator, are predefined on and cannot be changed. also provides some default sample roles, such as Resource Pool Administrator, that you can modify. You can create custom roles either from scratch or by cloning and modifying sample roles. See Create a vCenter Server Custom Role

The following figure illustrates how a permission is constructed from privileges and roles, and assigned to a user or group for a vSphere object.

Figure 84: vSphere Permissions



To assign permissions to an object, you follow these steps:

1. Select the object to which you want to apply the permission in thevCenter Server object hierarchy.
2. Select the group or user that should have privileges on the object.
3. Select individual privileges or a role, that is a set of privileges, that the group or user should have on the object.
   By default, Propagate to children is not selected. You must select the checkbox for the group or user to have the selected role on the selected object and its child objects.

vCenter Server offers sample roles, which combine frequently used privilege sets. You can also create custom roles by combining a set of roles.

Permissions must often be defined on both a source object and a destination object. For example, if you move a virtual machine, you need privileges on that virtual machine, but also privileges on the destination data center.

See the following information.

To find out about...	See...
Creating custom roles.	Create a vCenter Server Custom Role
All privileges and the objects to which you can apply the privileges	Defined Privileges
Sets of privileges that are required on different objects for different tasks.	Required vCenter Server Privileges for Common Tasks

The permissions model for standaloneESXi hosts is simpler. See Assigning Privileges for ESXi Hosts.

What IsvCenter Server User Validation

vCenter Server systems that use a directory service regularly validate users and groups against the user directory domain. Validation occurs at regular intervals specified in thevCenter Server settings. For example, assume that user Smith is assigned a role on several objects. The domain administrator changes the name to Smith2. The host concludes that Smith no longer exists and removes permissions associated with that user from the vSphere objects when the next validation occurs.

Similarly, if user Smith is removed from the domain, all permissions associated with that user are removed when the next validation occurs. If a new user Smith is added to the domain before the next validation occurs, the new user Smith replaces the old user Smith in permissions on any object.

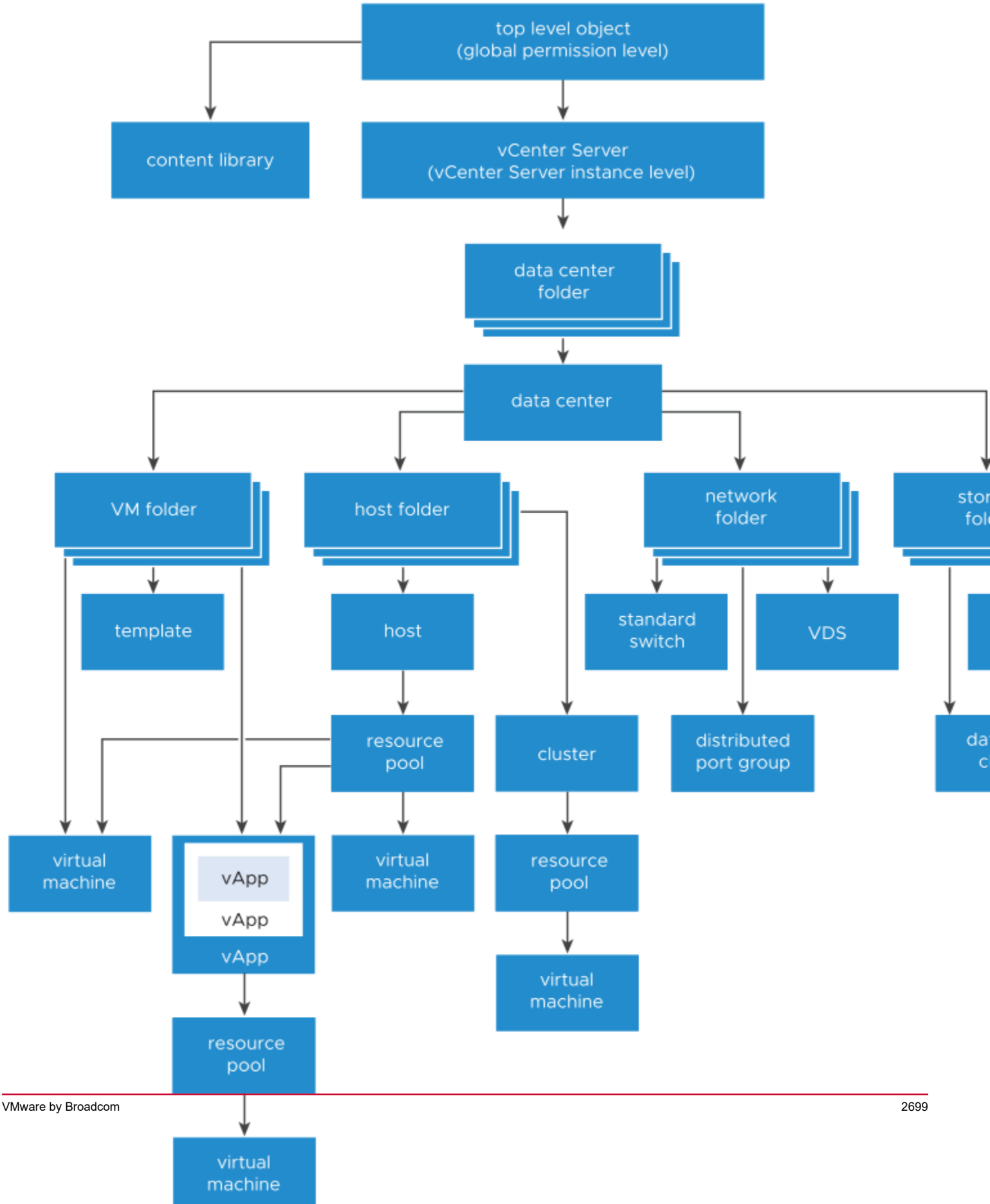
Hierarchical Inheritance of Permissions

When you assign a permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission. Propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

The following figure illustrates the inventory hierarchy and the paths by which permissions can propagate.

Note: Global permissions support assigning privileges across solutions from a global root object. See Global Permissions.

Figure 85: vSphere Inventory Hierarchy



About this figure:

- You cannot set direct permissions on the VM, host, network, and storage folders. That is, these folders act as containers, and as such are not visible to users.
- You cannot set permissions on standard switches.

Note: To be able to set and propagate permissions to children on a vSphere Distributed Switch (VDS), the switch object must reside in a network folder created on the data center.

Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent data center. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously.

For example, you can set permissions for a distributed switch and its associated distributed port groups, by setting permissions on a parent object, such as a folder or data center. You must also select the option to propagate these permissions to child objects.

Permissions take several forms in the hierarchy:

Managed entities	Managed entities refer to the following vSphere objects. Managed entities offer specific operations that vary depending on the entity type. Privileged users can define permissions on managed entities. See the vSphere API documentation for more information about vSphere objects, properties, and methods. • Clusters • Data centers • Datastores • Datastore clusters • Folders • Hosts • Networks (except vSphere Distributed Switches) • Distributed port groups • Resource pools • Templates • Virtual machines • vSphere vApps
Global entities	You cannot modify permissions on entities that derive permissions from the root vCenter Server system. • Custom fields • Licenses • Roles • Statistics intervals • Sessions

Multiple Permission Settings

Objects might have multiple permissions, but only one permission for each user or group. For example, one permission might specify that GroupAdmin has the Administrator role on an object. Another permission might specify that the GroupVMAdmin has the Virtual Machine Administrator role on the same object. However, the GroupVMAdmin group cannot have another permission for the same GroupVMAdmin on this object.

A child object inherits the permissions of its parent if the parent's propagate property is set to true. A permission that is set directly on a child object overrides the permission in the parent object. See Example 2: Child Permissions Overriding Parent Permissions.

If multiple group roles are defined on the same object, and a user belongs to two or more of those groups, two situations are possible:

- No permission for the user is defined directly on the object. In that case, the user gets the union of the permissions that the groups have on the object.
- A permission for the user is defined directly on the object. In that case, the permissions for the user take precedence over all group permissions.

Example 1: Permission Inheritance from Multiple Groups

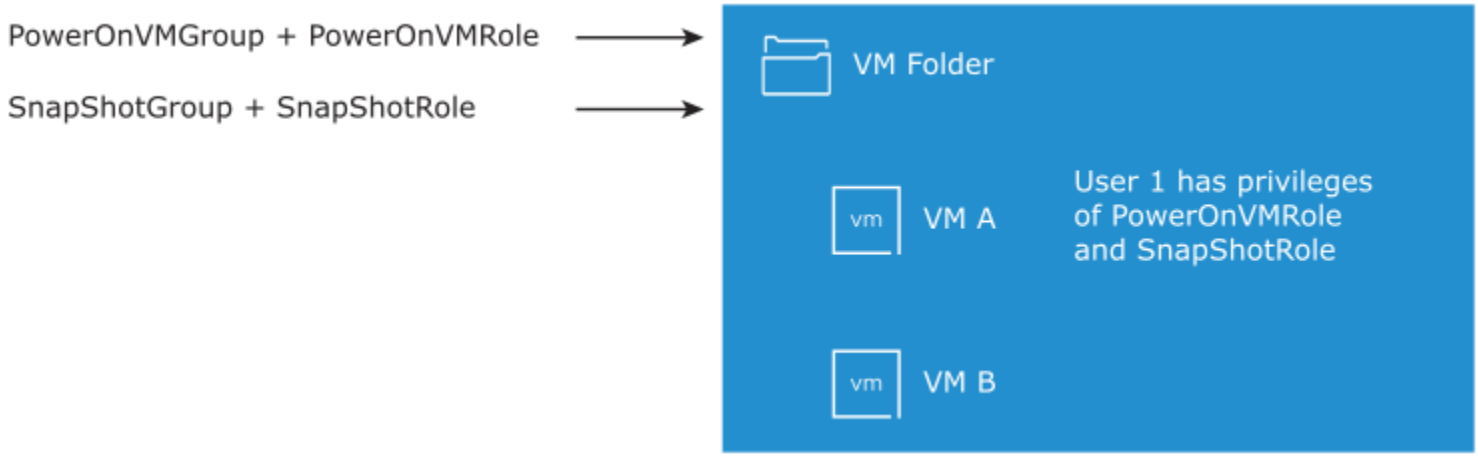
This example illustrates how an object can inherit multiple permissions from groups that are granted permission on a parent object.

In this example, two permissions are assigned on the same object for two different groups.

- PowerOnVMRole can power on virtual machines.
- SnapShotRole can take snapshots of virtual machines.
- PowerOnVMGroup is granted the PowerOnVMRole on VM Folder, with the permission set to propagate to child objects.
- SnapShotGroup is granted the SnapShotRole on VM Folder, with the permission set to propagate to child objects.
- User 1 is not assigned specific privileges.

User 1, who belongs to both the PowerOnVMGroup and the SnapShotGroup, logs in. User 1 can both power on and take snapshots of both VM A and VM B.

Figure 86: Example 1: Permission Inheritance from Multiple Groups



Example 2: Child Permissions Overriding Parent Permissions

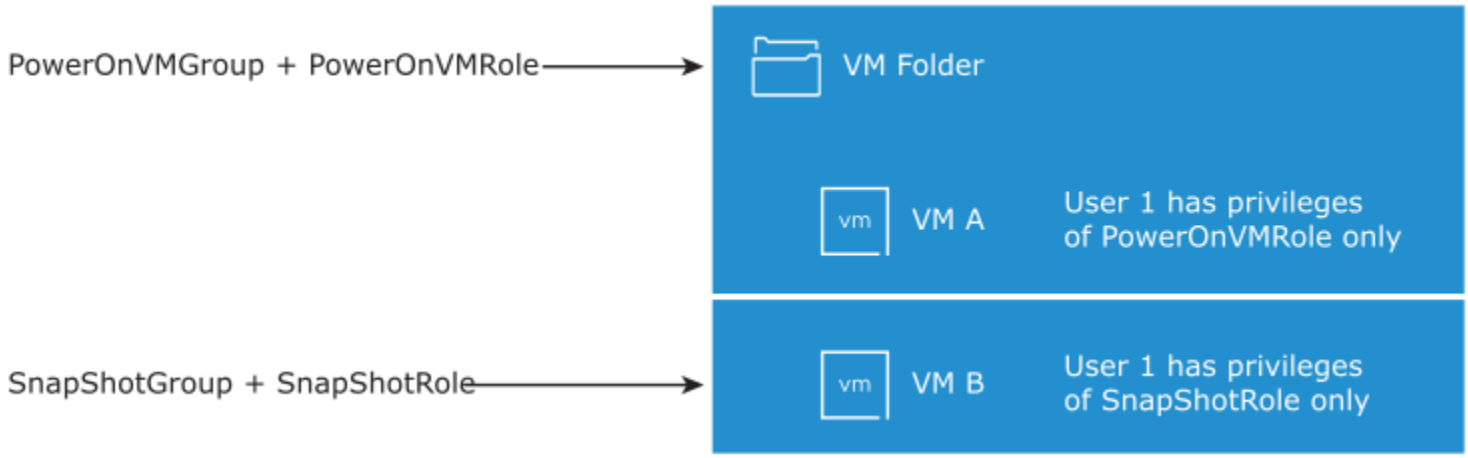
This example illustrates how permissions that are assigned on a child object can override permissions that are assigned on a parent object. You can use this overriding behavior to restrict user access to particular areas of the inventory.

In this example, permissions are defined on two different objects for two different groups.

- PowerOnVMRole can power on virtual machines.
- SnapShotRole can take snapshots of virtual machines.
- PowerOnVMGroup is granted the PowerOnVMRole on VM Folder, with the permission set to propagate to child objects.
- SnapShotGroup is granted the SnapShotRole on VM B.

User 1, who belongs to both the PowerOnVMGroup and the SnapShotGroup, logs in. Because the SnapShotRole is assigned at a lower point in the hierarchy than the PowerOnVMRole, it overrides PowerOnVMRole on VM B. User 1 can power on VM A, but not take snapshots. User 1 can take snapshots of VM B, but not power it on.

Figure 87: Example 2: Child Permissions Overriding Parent Permissions



Example 3: User Role Overriding Group Role

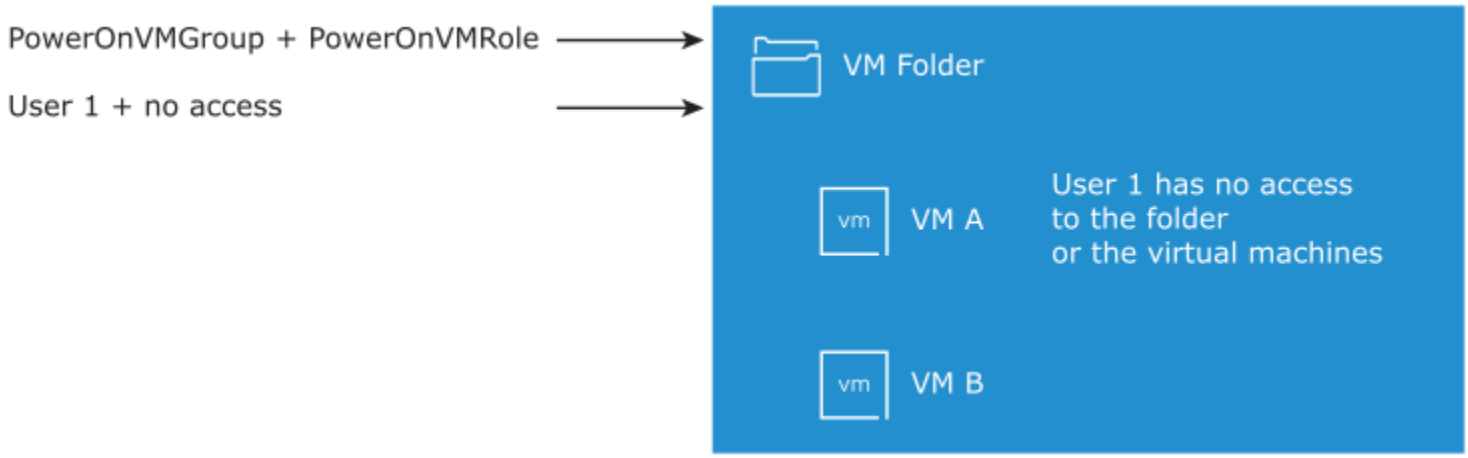
This example illustrates how the role assigned directly to an individual user overrides the privileges associated with a role assigned to a group.

In this example, permissions are defined on the same object. One permission associates a group with a role, the other permission associates an individual user with a role. The user is a member of the group.

- PowerOnVMRole can power on virtual machines.
- PowerOnVMGroup is granted the PowerOnVMRole on VM Folder.
- User 1 is granted the NoAccess role on VM Folder.

User 1, who belongs to PowerOnVMGroup, logs in. The NoAccess role granted to User 1 on VM Folder overrides the role assigned to the group. User 1 has no access to VM Folder or VMs A and B. VMs A and B are not visible in the hierarchy to User 1.

Figure 88: Example 3: User Permissions Overriding Group Permissions



Managing Permissions for vCenter Components

A permission is set on an object in the vCenter object hierarchy. Each permission associates the object with a group or user and the group's or user's access role. For example, you can select a virtual machine object, add one permission that gives the ReadOnly role to Group 1, and add a second permission that gives the Administrator role to User 2.

By assigning a different role to a group of users on different objects, you control the tasks that those users can perform in your vSphere environment. For example, to allow a group to configure memory for the host, select that host and add a permission that grants a role to that group that includes the**Host** > **Configuration** > **Memory Configuration** privilege.

For conceptual information about permissions, see the discussion in Understanding the Object-Level Permission Model.

You can assign permissions to objects at different levels of the hierarchy, for example, you can assign permissions to a host object or to a folder object that includes all host objects. See Hierarchical Inheritance of Permissions. You can also assign propagating permissions to a global root object to apply the permissions to all object in all solutions. See Global Permissions.

Add a Permission to an Inventory Object

After you create users and groups and define roles, you must assign the users and groups and their roles to the relevant inventory objects. You can assign the same propagating permissions to multiple objects simultaneously by moving the objects into a folder and setting the permissions on the folder.

On the object whose permissions you want to modify, you must have a role that includes the **Permissions** > **Modify permission** privilege.

When you assign permissions, the user and the group names must match Active Directory precisely, including case. If you upgraded from earlier versions of vSphere, check for case inconsistencies if you experience problems with groups.

1. Browse to the object for which you want to assign permissions in the vSphere Client object navigator.
2. Click the **Permissions** tab.
3. Click **Add**.
4. Optional: If you have configured an external identity provider for federated authentication, the domain of that identity provider is available to select in the **Domain** drop-down menu.
5. Select the user or group that will have the privileges defined by the selected role.
   a) From the **Domain** drop-down menu, select the domain for the user or group.
   b) Enter a name in the Search box.
      The system searches user names and group names.
   c) Select the user or group.
6. Select a role from the **Role** drop-down menu.
7. Optional: To propagate the permissions, select the **Propagate to children** check box.
   The role is applied to the selected object and propagates to the child objects.

8. Click **OK**.

Change or Remove Permissions

After a user or group and role pair is set for an inventory object, you can change the role paired with the user or group or change the setting of the **Propagate to children** check box. You can also remove the permission setting.

1. Browse to the object in the vSphere Client object navigator.
2. Click the **Permissions** tab.
3. Click a row to select a permission.

Task	Steps
Change permissions	1. Click the **Change Role** icon. 2. Select a role for the user or group from the **Role** drop-down menu. 3. Toggle the **Propagate to children** check box to change permission inheritance. 4. Click **OK**.
Remove permissions	Click the **Remove Permission** icon.

Change User Validation Settings

vCenter Server periodically validates its user and group lists against the users and groups in the user directory. It then removes users or groups that no longer exist in the domain. You can disable validation or change the interval between validations. If you have domains with thousands of users or groups, or if searches take a long time to complete, consider adjusting the search settings.

ForvCenter Server versions beforevCenter Server 5.0, these settings apply to an Active Directory associated withvCenter Server. ForvCenter Server 5.0 and later, these settings apply tovCenter Single Sign-On identity sources.

Note: This procedure applies only tovCenter Server user lists. You cannot searchESXi user lists in the same way.

1. Browse to thevCenter Server system in thevSphere Client object navigator.
2. Select **Configure** and click **Settings** > **General**.
3. Click **Edit** and select **User directory**.
4. Change the values as needed and click **Save**.

Option	Description
User directory timeout	Timeout interval, in seconds, for connecting to the Active Directory server. This value specifies the maximum amount of timevCenter Server allows a search to run on the selected domain. Searching large domains can take a long time.
Query limit	Toggle on to set a maximum number of users and groups thatvCenter Server displays.
Query limit size	Maximum number of users and groups from the selected domain thatvCenter Server displays in the **Select Users or Groups** dialog box. If you enter 0 (zero), all users and groups appear.

Global Permissions

Global permissions are applied to a global root object that spans solutions. In an on-premises SDDC, global permissions might span bothvCenter Server and vRealize Orchestrator. But for any vSphere SDDC, global permissions apply to global objects such as tags and content libraries.

You can assign global permissions to users or groups, and decide on the role for each user or group. The role determines the set of privileges that the user or group has for all objects in the hierarchy. You can assign a predefined role or create custom roles. See Using Roles to Assign Privileges.

It is important to distinguish betweenvCenter Server permissions and global permissions.

vCenter Server permissions	You usually apply a permission to avCenter Server inventory object such as a virtual machine. When you do, you specify that a user or group has a role (set of privileges) on the object.
Global permissions	Global permissions give a user or group privileges to view or manage all objects in each of the inventory hierarchies in your deployment. Global permissions also apply to global objects such as tags and content libraries. See Permissions on Tag Objects. If you assign a global permission and do not select Propagate, the users or groups associated with this permission do not have access to the objects in the hierarchy. They only have access to some global functionality such as creating roles.

Important: Use global permissions with care. Verify that you really want to assign permissions to all objects in all inventory hierarchies.

Add a Global Permission

You can use global permissions to give a user or group privileges for all objects in all inventory hierarchies in your deployment.

To perform this task, you must have **Permissions** > **Modify permission** privileges on the root object for all inventory hierarchies.

Important: Use global permissions with care. Verify that you really want to assign permissions to all objects in all inventory hierarchies.

1. Log in to the vCenter Server by using the vSphere Client.
2. Select **Administration** and click **Global Permissions** in the Access Control area.
3. Select the domain from the **Permissions provider** drop-down menu.
4. Optional: If you have configured an external identity provider for federated authentication, the domain of that identity provider is available to select in the **Domain** drop-down menu.
5. Click **Add**.
6. Select the user or group that will have the privileges defined by the selected role.
   a) From the **Domain** drop-down menu, select the domain for the user or group.
   b) Enter a name in the Search box.
      The system searches user names and group names.
   c) Select the user or group.
7. Select a role from the **Role** drop-down menu.
8. Decide whether to propagate the permissions by selecting the **Propagate to children** check box.
   If you assign a global permission and do not select **Propagate to children**, the users or groups associated with this permission do not have access to the objects in the hierarchy. They only have access to some global functionality such as creating roles.

9. Click **OK**.

Permissions on Tag Objects

In the vCenter Server object hierarchy, tag objects are not children of vCenter Server but are created at the vCenter Server top level. In environments with multiple vCenter Server instances, tag objects are shared across vCenter Server instances. Permissions for tag objects work differently than permissions for other objects in the vCenter Server object hierarchy.

Only Global Permissions or Permissions Assigned to the Tag Object Apply

If you grant permissions to a user on a vCenter Server inventory object, such as a virtual machine, that user can perform the tasks associated with the permission. However, the user cannot perform tag operations on the object.

For example, if you grant the **Assign vSphere Tag** privilege to user Dana on host TPA, that permission does not affect whether Dana can assign tags on host TPA. Dana must have the **Assign vSphere Tag** privilege at the top level, that is, a global permission, or must have the privilege for the tag object.

Table 233: How Global Permissions and Tag Object Permissions Affect What Users Can Do

Global Permission	Tag-Level Permission	vCenter Server Object-Level Permission	Effective Permission
No tagging privileges assigned.	Dana has **Assign or Unassign vSphere Tag** privileges for the tag.	Dana has **Delete vSphere Tag** privileges on ESXi host TPA.	Dana has **Assign or Unassign vSphere Tag** privileges for the tag.
Dana has **Assign or Unassign vSphere Tag** privileges.	No privileges assigned for the tag.	Dana has **Delete vSphere Tag** privileges on ESXi host TPA.	Dana has **Assign or Unassign vSphere Tag** global privileges. That includes privileges at the tag level.
No tagging privileges assigned.	No privileges assigned for the tag.	Dana has **Assign or Unassign vSphere Tag** privileges on ESXi host TPA.	Dana does not have tagging privileges on any object, including host TPA.

Global Permissions Complement Tag Object Permissions

Global permissions, that is, permissions that are assigned on the top-level object, complement permissions on tag objects when the permissions on the tag objects are more restrictive. The vCenter Server permissions do not affect the tag objects.

For example, assume that you assign the **Delete vSphere Tag** privilege to user Robin at the top level by using global permissions. For the tag Production, you do not assign the **Delete vSphere Tag** privilege to Robin. In that case, Robin has the privilege for the tag Production because Robin has the global permission, which propagates from the top level. You cannot restrict privileges unless you modify the global permission.

Table 234: Global Permissions Complement Tag-Level Permissions

Global Permission	Tag-Level Permission	Effective Permission
Robin has **Delete vSphere Tag** privileges	Robin does not have **Delete vSphere Tag** privileges for the tag.	Robin has **Delete vSphere Tag** privileges.

Global Permission	Tag-Level Permission	Effective Permission
No tagging privileges assigned	Robin does not have **Delete vSphere Tag** privileges assigned for the tag.	Robin does not have **Delete vSphere Tag** privileges

Tag-Level Permissions Can Extend Global Permissions

You can use tag-level permissions to extend global permissions. That means users can have both a global permission and a tag-level permission on a tag.

Note: This behavior is different from how vCenter Server privileges are inherited. In vCenter Server, permissions defined for a child object always override the permissions that are propagated from parent objects.

Table 235: Global Permissions Extend Tag-Level Permissions

Global Permission	Tag-Level Permission	Effective Permission
Lee has **Assign or Unassign vSphere Tag** privilege.	Lee has **Delete vSphere Tag** privilege.	Lee has the **Assign vSphere Tag** privilege and the **Delete vSphere Tag** privilege for the tag.
No tagging privileges assigned.	Lee has **Delete vSphere Tag** privilege assigned for the tag.	Lee has the **Delete vSphere Tag** privilege for the tag.

Using Roles to Assign Privileges

A role is a predefined set of privileges. Privileges define rights to perform actions and read properties. For example, the Virtual Machine Administrator role allows a user to read and change virtual machine attributes.

When you assign permissions, you pair a user or group with a role and associate that pairing with an inventory object. A single user or group can have different roles for different objects in the inventory.

For example, assume that you have two resource pools in your inventory, Pool A and Pool B. You can assign group Sales the Virtual Machine User role on Pool A, and the Read Only role on Pool B. With these assignments, the users in group Sales can turn on virtual machines in Pool A, but can only view virtual machines in Pool B.

vCenter Server provides system roles and sample roles by default.

System roles
System roles are permanent. You cannot edit the privileges associated with these roles.

Sample roles
VMware provides sample roles for certain frequently performed combination of tasks. You can clone, modify, or remove these roles.

Note: To avoid losing the predefined settings in a sample role, clone the role first and make modifications to the clone. You cannot reset the sample to its default settings.

Users can schedule tasks only if they have a role that includes privileges to perform that task at the time the task is created.

Note: Changes to roles and privileges take effect immediately, even if the users involved are logged in. The exception is searches, where changes take effect after the user has logged out and logged back in.

Custom Roles in vCenter Server and ESXi

You can create custom roles for vCenter Server and all objects that it manages, or for individual hosts.

vCenter Server Custom Roles (Recommended)	Create custom roles by using the role-editing facilities in the vSphere Client to create privilege sets that match your needs.
ESXi Custom Roles	You can create custom roles for individual hosts by using a CLI or the VMware Host Client. See the *vSphere Single Host Management - VMware Host Client* documentation. Custom host roles are not accessible from vCenter Server. If you manage ESXi hosts through vCenter Server, do not maintain custom roles in both the host and vCenter Server. Define roles at the vCenter Server level.

When you manage a host using vCenter Server, the permissions associated with that host are created through vCenter Server and stored on vCenter Server. If you connect directly to a host, only the roles that are created directly on the host are available.

Note: When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: **System** > **Anonymous**, **System** > **View**, and **System** > **Read**. These privileges are not visible in the vSphere Client but are used to read certain properties of some managed objects. All the predefined roles in vCenter Server contain these three system-defined privileges. See the *vSphere Web Services API* documentation for more information.

Create a vCenter Server Custom Role

To suit the access control needs of your environment, you can create vCenter Server custom roles. You can create a role or clone an existing role.

Verify that you are logged in as a user with Administrator privileges.

You can create or edit a role on a vCenter Server system that is part of the same vCenter Single Sign-On domain as other vCenter Server systems. The VMware Directory Service (vmdir) propagates the role changes that you make to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across vCenter Server systems.

1. Log in to the vCenter Server by using the vSphere Client.
2. Select **Administration** and click **Roles** in the **Access Control** area.
3. Create the role:

Option	Description
To create a role	Click **New**.
To create the role by cloning	Select a role, and click **Clone**.

   See vCenter Server System Roles for more information.
4. Enter a name for the new role.
5. Select and deselect privileges for the role.

   Scroll the privilege categories and select all privileges or a subset of privileges for that category. You can show all, selected, or unselected categories. You can also show all, selected, or unselected privileges.

   See Defined Privileges for more information.

   Note: When creating a cloned role, you cannot change privileges. To change privileges, select the cloned role and click **Edit**.
6. Click **Add**.

You can now create permissions by selecting an object and assigning the role to a user or group for that object.

vCenter Server System Roles

A role is a predefined set of privileges. When you add permissions to an object, you pair a user or group with a role.vCenter Server includes some default system roles, which you cannot change.

vCenter Server provides a few default roles. You cannot change the privileges associated with the default roles. The default roles are organized as a hierarchy. Each role inherits the privileges of the previous role. For example, the Administrator role inherits the privileges of the Read Only role.

To view the privileges associated with a default role, navigate to the role in the vSphere Client (**Menu** > **Administration** > **Roles**) and click the **Privileges** tab.

To view all the vSphere privileges and descriptions, see Defined Privileges.

ThevCenter Server role hierarchy also includes several sample roles. You can clone a sample role to create a similar role.

If you create a role, it does not inherit privileges from any of the system roles.

Administrator Role	Users with the Administrator role for an object are allowed to view and perform all actions on the object. This role also includes all privileges of the Read Only role. If you have the Administrator role on an object, you can assign privileges to individual users and groups. If you are acting in the Administrator role invCenter Server, you can assign privileges to users and groups in the defaultvCenter Single Sign-On identity source. See the *vSphere Authentication* documentation for supported identity services. By default, the administrator@vsphere.local user has the Administrator role on bothvCenter Single Sign-On andvCenter Server after installation. That user can then associate other users with the Administrator role onvCenter Server.
Read Only Role	Users with the Read Only role for an object are allowed to view the state of the object and details about the object. For example, users with this role can view virtual machine, host, and resource pool attributes, but cannot view the remote console for a host. All actions through the menus and toolbars are disallowed.
No Access Role	Users with the No Access role for an object cannot view or change the object in any way. New users and groups are assigned this role by default. You can change the role on an object-by-object basis. The administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, the root user, and vpxuser are assigned the Administrator role by default. Other users are assigned the No Access role by default.

Best practice is to create a user at the root level and assign the Administrator role to that user. After creating a named user with Administrator privileges, you can remove the root user from any permissions or change its role to No Access.

Best Practices for Roles and Permissions

Follow best practices for roles and permissions to maximize the security and manageability of your vCenter Server environment.

Follow these best practices when configuring roles and permissions in your vCenter Server environment:

- Where possible, assign a role to a group rather than individual users.

- Grant permissions only on the objects where they are needed, and assign privileges only to users or groups that must have them. Use the minimum number of permissions to make it easier to understand and manage your permissions structure.
- If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users with administrative privileges. Otherwise, you might unintentionally restrict administrators' privileges in the parts of the inventory hierarchy where you have assigned that group the restrictive role.
- Use folders to group objects. For example, to grant modify permission on one set of hosts and view permission on another set of hosts, place each set of hosts in a folder.
- Consider enabling propagation when you assign permissions to an object. Propagation ensures that new objects in the object hierarchy inherit permissions. For example, you can assign a permission to a virtual machine folder and enable propagation to ensure that the permission applies to all VMs in the folder.
- Use the No Access role to mask specific areas of the hierarchy. The No Access role restricts access for the users or groups with that role.

Required vCenter Server Privileges for Common Tasks

Many tasks require permissions on multiple objects in the vSphere inventory. If the user who attempts to perform the task only has privileges on one object, the task cannot complete successfully.

The following table lists common tasks that require more than one privilege. You can add permissions to inventory objects by pairing a user with one of the predefined roles or with multiple privileges. If you expect that you must assign a set of privileges multiple times, create custom roles. To learn more about required privileges for common tasks, see Privilege Recorder.

Refer to the *vSphere Web Services API Reference* documentation to learn how operations in the vSphere Client user interface map to API calls, and what privileges are required to perform operations. For example, the API documentation for the `AddHost_Task(addHost)` method specifies that the Host.Inventory.AddHostToCluster privilege is required to add a host to a cluster.

If the task that you want to perform is not in this table, the following rules explain where you must assign permissions to allow particular operations:

- Any operation that consumes storage space requires the **Datastore** > **Allocate Space** privilege on the target datastore, and the privilege to perform the operation itself. You must have these privileges, for example, when creating a virtual disk or taking a snapshot.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource** > **Assign Virtual Machine to Resource Pool** privilege.

Table 236: Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center: • **Virtual machine** > **Inventory** > **Create new** • **Virtual machine** > **Configuration** > **Add new disk** (if creating a new virtual disk) • **Virtual machine** > **Configuration** > **Add existing disk** (if using an existing virtual disk) • **Virtual machine** > **Configuration** > **Configure Raw device** (if using an RDM or SCSI pass-through device)	Administrator

Task	Required Privileges	Applicable Role
	On the destination host, cluster, or resource pool: **Resource** > **Assign virtual machine to resource pool**	Resource pool administrator or Administrator
	On the destination datastore or the folder that contains the datastore: **Datastore** > **Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network** > **Assign network**	Network Consumer or Administrator
Power on a virtual machine	On the data center in which the virtual machine is deployed: **Virtual machine** > **Interaction** > **Power On**	Virtual Machine Power User or Administrator
	On the virtual machine or folder of virtual machines: **Virtual machine** > **Interaction** > **Power On**	
Deploy a virtual machine from a template	On the destination folder or data center: • **Virtual machine** > **Inventory** > **Create from existing** • **Virtual machine** > **Configuration** > **Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine** > **Provisioning** > **Deploy template**	Administrator
	On the destination host, cluster or resource pool: • **Resource** > **Assign virtual machine to resource pool** • **vApp** > **Import**	Administrator
	On the destination datastore or folder of datastores: **Datastore** > **Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network** > **Assign network**	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual machine** > **Snapshot management** > **Create snapshot**	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: • **Resource** > **Assign virtual machine to resource pool** • **Virtual machine** > **Inventory** > **Move**	Administrator
	On the destination resource pool: **Resource** > **Assign virtual machine to resource pool**	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: • **Virtual machine** > **Interaction** > **Answer question** • **Virtual machine** > **Interaction** > **Console interaction** • **Virtual machine** > **Interaction** > **Device connection** • **Virtual machine** > **Interaction** > **Power Off** • **Virtual machine** > **Interaction** > **Power On** • **Virtual machine** > **Interaction** > **Reset** • **Virtual machine** > **Interaction** > **Configure CD media** (if installing from a CD) • **Virtual machine** > **Interaction** > **Configure floppy media** (if installing from a floppy disk) • **Virtual machine** > **Interaction** > **VMware Tools install**	Virtual Machine Power User or Administrator
	On a datastore that contains the installation media ISO image: **Datastore** > **Browse datastore** (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image:	Virtual Machine Power User or Administrator

Task	Required Privileges	Applicable Role
	• **Datastore** > **Browse datastore** • **Datastore** > **Low level file operations** • **Host** > **Configuration** > **System Management**	
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: • **Resource** > **Migrate powered on virtual machine** • **Resource** > **Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource** > **Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: • **Resource** > **Migrate powered off virtual machine** • **Resource** > **Assign virtual machine to resource pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource** > **Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): **Datastore** > **Allocate space**	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource** > **Migrate powered on virtual machine**	Resource Pool Administrator or Administrator
	On the destination datastore: **Datastore** > **Allocate space**	Datastore Consumer or Administrator
On the destination cluster: • **Host** > **Inventory** > **Add host to cluster** • **Host** > **Inventory** > **Modify cluster**	Administrator	Administrator
Add a single host to a data center by using the vSphere Client, or add a single host to a cluster by using PowerCLI or API (leveraging the addHost API)	On the host: **Host** > **Inventory** > **Add host to cluster**	
	On the cluster: • **Host** > **Inventory** > **Modify cluster** • **Host** > **Inventory** > **Add host to cluster**	Administrator
	On the data center: **Host** > **Inventory** > **Add standalone host**	Administrator
Add multiple hosts to a cluster	On the cluster: • **Host** > **Inventory** > **Modify cluster** • **Host** > **Inventory** > **Add host to cluster**	Administrator
	On the parent data center of the cluster (with propagate): • **Host** > **Inventory** > **Add standalone host** • **Host** > **Inventory** > **Move host** • **Host** > **Inventory** > **Modify cluster** • **Host** > **Configuration** > **Maintenance**	Administrator
Encrypt a virtual machine		Administrator

Task	Required Privileges	Applicable Role
Protect a virtual machine (if using vSphere+ to protect the virtual machine)	On the data center in which the virtual machine is deployed: • **vSphere Tagging** > **Assign or Unassign vSphere Tag**	Administrator

Securing ESXi Hosts

The ESXi hypervisor architecture has many built-in security features such as CPU isolation, memory isolation, and device isolation. You can configure additional features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.

An ESXi host is also protected with a firewall. You can open ports for incoming and outgoing traffic as needed, but should restrict access to services and ports. Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment. ESXi hosts participate in the certificate infrastructure. Hosts are provisioned with certificates that are signed by the VMware Certificate Authority (VMCA) by default.

See the VMware white paper *Security of the VMware vSphere Hypervisor* for additional information on ESXi security.

Note:

ESXi is not built upon the Linux kernel or a commodity Linux distribution. It uses its own VMware specialized and proprietary kernel and software tools, delivered as a self-contained unit, and does not contain applications and components from Linux distributions.

General ESXi Security Recommendations

To protect an ESXi host against an unauthorized intrusion and misuse, VMware imposes constraints on several parameters, settings, and activities. You can loosen the constraints to meet your configuration needs. If you do, make sure that you are working in a trusted environment and take other security measures.

Built-In Security Features

Risks to the hosts are mitigated as follows:

- ESXi Shell and SSH interfaces are disabled by default. Keep these interfaces disabled unless you are performing troubleshooting or support activities. For day-to-day activities, use the vSphere Client, where activity is subject to role-based access control and modern access control methods.
- Only a limited number of firewall ports are open by default. You can explicitly open additional firewall ports that are associated with specific services.
- ESXi runs only services that are essential to managing its functions. The distribution is limited to the features required to run ESXi.
- By default, all ports that are not required for management access to the host are closed. Open ports if you need additional services.
- By default, weak ciphers are disabled and communications from clients are secured by SSL. The exact algorithms used for securing the channel depend on the SSL handshake. Default certificates created on ESXi use PKCS#1 SHA-256 with RSA encryption as the signature algorithm.
- An internal web service is used by ESXi to support access by Web clients. The service has been modified to run only functions that a Web client requires for administration and monitoring. As a result, ESXi is not vulnerable to web service security issues reported in broader use.
- VMware monitors all security alerts that can affect ESXi security and issues a security patch if needed. You can subscribe to the VMware Security Advisories and Security Alerts mailing list to receive security alerts. See the webpage at http://lists.vmware.com/mailman/listinfo/security-announce.
- Insecure services such as FTP and Telnet are not installed, and the ports for these services are closed by default.

- To protect hosts from loading drivers and applications that are not cryptographically signed, use UEFI Secure boot. Enabling Secure Boot is done at the system BIOS. No additional configuration changes are required on the ESXi host, for example, to disk partitions. See UEFI Secure Boot for ESXi Hosts.
- If your ESXi host has a TPM 2.0 chip, enable and configure the chip in the system BIOS. Working together with Secure Boot, TPM 2.0 provides enhanced security and trust assurance rooted in hardware. See Securing ESXi Hosts with Trusted Platform Module.

Additional Security Measures

Consider the following recommendations when evaluating host security and administration.

Limit access	If you enable access to the Direct Console User Interface (DCUI), the ESXi Shell, or SSH, enforce strict access security policies. The ESXi Shell has privileged access to certain parts of the host. Provide only trusted users with ESXi Shell login access.
Do not access managed hosts directly	Use the vSphere Client to administer ESXi hosts that are managed by a vCenter Server. Do not access managed hosts directly with the VMware Host Client, and do not change managed hosts from the DCUI. If you manage hosts with a scripting interface or API, do not target the host directly. Instead, target the vCenter Server system that manages the host and specify the host name.
Use DCUI only for troubleshooting	Access the host from the DCUI or the ESXi Shell as the root user only for troubleshooting. To administer your ESXi hosts, use one of the GUI clients, or one of the VMware CLIs or APIs. See *ESXCLI Concepts and Examples* at https://code.vmware.com/. If you use the ESXi Shell or SSH, limit the accounts that have access and set timeouts.
Use only VMware sources to upgrade ESXi components	The host runs several third-party packages to support management interfaces or tasks that you must perform. VMware only supports upgrades to these packages that come from a VMware source. If you use a download or patch from another source, you might compromise management interface security or functions. Check third-party vendor sites and the VMware knowledge base for security alerts.

Note: Follow the VMware security advisories at http://www.vmware.com/security/.

Advanced System Settings

Advanced system settings control aspects of ESXi behavior, such as logging, system resources, and security.

The following table presents some of the important ESXi advanced system settings for security. To view all the advanced system settings, consult either the vSphere Client (**Host** > **Configure** > **System** > **Advanced System Settings)** or the API for a given release.

Table 237: Partial List of Security Advanced System Settings

Advanced System Setting	Description	Default Value
Annotations.WelcomeMessage	Displays a welcome message in the Host Client prior to login, or in the DCUI on the default screen. In the DCUI, the welcome message replaces some text, such as the host IP address.	(Empty)
Config.Etc.issue	Displays a banner during an SSH login session. Use a trailing newline for best results.	(Empty)
Config.Etc.motd	Displays the message of the day upon SSH login.	(Empty)
Config.HostAgent.vmacore.soap.sessionTimeout	Sets the idle time in minutes before the system automatically logs out a VIM API. A value of 0 (zero) deactivates the idle time. This setting applies only to new sessions.	30 (minutes)
Mem.MemEagerZero	Activates zeroing the user world and the guest memory pages in the VMkernel operating systems (including the VMM process) after a virtual machine exit. The default value (0) uses lazy zeroing. A value of 1 uses eager zeroing.	0 (deactivated)
Security.AccountLockFailures	Sets the maximum number of failed login attempts before the system locks a user's account. For example, to lock the account on the fifth login failure, set this value to 4. A value of 0 (zero) deactivates account locking. For implementation reasons, some login mechanisms count unexpectedly: • VIM logins (including the VMware Host Client) and ESXCLI reflect the exact number of failed logins. • SSH connections count as a login attempt when displaying a password prompt, and undo that count on successful login. This behavior is normal for challenge and response communications. • CGI logins double-count login failures. **CAUTION:** Due to this problem, a user can be locked out faster than the number of failed logins when using the CGI interface.	5
Security.AccountUnlockTime	Sets the number of seconds that a user is locked out. Any login attempt within the specified lock timeout restarts the lock timeout.	900 (15 minutes)

Advanced System Setting	Description	Default Value
Security.PasswordHistory	Sets the number of passwords to remember for each user. This setting prevents duplicate or similar passwords.	0
Security.PasswordMaxDays	Sets the maximum number of days between password changes.	99999
Security.PasswordQualityControl	Changes the required length and the character class requirement or allow pass phrases in the `Pam_passwdqc` configuration. You can use special characters in passwords. You can have password lengths of at least 15 characters. The default setting requires three character classes and a minimum length of seven characters. If implementing the DoD Annex, you can combine the `similar=deny` option plus a minimum password length to enforce a requirement that passwords are sufficiently different. The password history setting is only enforced for passwords changed through the VIM `LocalAccountManager.changePassword` API. To change the password requires that the user have administrator permission. The PasswordQualityControl setting, with a PasswordMaxDays setting, satisfies the requirements of the DoD Annex: `min=disabled,disabled,disabled,disabled,15 similar=deny`	retry=3 min=disabled,disabled,disabled,7,7
UserVars.DcuiTimeOut	Sets the idle time in seconds before the system automatically logs out the DCUI. A value of 0 (zero) deactivates the timeout.	600 (10 minutes)
UserVars.ESXiShellInteractiveTimeOut	Sets the idle time in seconds before the system automatically logs out an interactive shell. This setting takes effect for new sessions only. A value of 0 (zero) deactivates the idle time. Applies to both the DCUI and the SSH shell.	0
UserVars.ESXiShellTimeOut	Sets the time in seconds a login shell waits for login. A value of 0 (zero) deactivates the timeout. Applies to both the DCUI and the SSH shell.	0
UserVars.HostClientSessionTimeout	Sets the idle time in seconds before the system automatically logs out the Host Client. A value of 0 (zero) deactivates the idle time.	900 (15 minutes)
UserVars.HostClientWelcomeMessage	Displays a welcome message in the Host Client upon login. The message is displayed following login as a “hint”.	(Empty)

Configure ESXi Hosts with Host Profiles

Host profiles allow you to set up standard configurations for your ESXi hosts and automate compliance to these configuration settings. Host profiles allow you to control many aspects of host configuration including memory, storage, networking, and so on.

You can configure host profiles for a reference host from the vSphere Client and apply the host profile to all hosts that share the characteristics of the reference host. You can also use host profiles to monitor hosts for host configuration changes. See *vSphere Host Profiles* documentation.

You can attach the host profile to a cluster to apply it to all hosts in the cluster.

1. Set up the reference host to specification and create a host profile.
2. Attach the profile to a host or cluster.
3. Apply the host profile of the reference host to other hosts or clusters.

Use Scripts to Manage Host Configuration Settings

In environments with many hosts, managing hosts with scripts is faster and less error prone than managing the hosts from the vSphere Client.

vSphere includes several scripting languages for host management. See *ESXCLI Documentation* and *vSphere API/SDK Documentation* for reference information and programming tips, and VMware Communities for additional tips about scripted management. The vSphere Administrator documentation focuses on using the vSphere Client for management.

VMware PowerCLI	VMware PowerCLI is a Windows PowerShell interface to the vSphere API. VMware PowerCLI includes PowerShell cmdlets for administering vSphere components. VMware PowerCLI includes hundreds of cmdlets, a set of sample scripts, and a function library for management and automation. See https://developer.vmware.com/powercli.
ESXCLI	ESXCLI includes a set of commands for managing ESXi hosts and virtual machines. See *ESXCLI Documentation*.

You can also use one of the scripting interfaces to the vSphere Automation SDK such as the vSphere Automation SDK for Python.

1. Create a custom role that has limited privileges.

   For example, consider creating a role that has a set of privileges for managing hosts but no privileges for managing virtual machines, storage, or networking. If the script you want to use only extracts information, you can create a role with read-only privileges for the host.
2. From the vSphere Client, create a service account and assign it the custom role.

   You can create multiple custom roles with different levels of access if you want access to certain hosts to be fairly limited.
3. Write scripts to perform parameter checking or modification, and run them.

   For example, you can check or set the shell interactive timeout of a host as follows:

Language	Commands
ESXCLI	`esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeOut` `esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut`

Language	Commands

PowerCLI	`#List UserVars.ESXiShellInteractiveTimeOut for each host`
	`Get-VMHost | Select Name,`
	`@{N="UserVars.ESXiShellInteractiveTimeOut";E={$_`
	`| Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut`
	`| Select -ExpandProperty Value}}`
	
	`# Set UserVars.ESXiShellTimeOut to 900 on all hosts`
	`Get-VMHost`
	`| Foreach { Get-AdvancedSetting -Entity $_ -Name UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -Value 900 }`

4. In large environments, create roles with different access privileges and group hosts into folders according to the tasks that you want to perform. You can then run scripts over different folders from different service accounts.
5. Verify that the changes happened after you run the command.

ESXi Passwords and Account Lockout

For ESXi hosts, you must use a password with predefined requirements. You can change the required length and character class requirement or allow pass phrases using the Security.PasswordQualityControl advanced option. You can also set the number of passwords to remember for each user using the Security.PasswordHistory advanced option.

Note: The default requirements for ESXi passwords can change from one release to the next. You can check and change the default password restrictions by using the Security.PasswordQualityControl advanced option.

ESXi Passwords

ESXi enforces password requirements for access from the Direct Console User Interface, the ESXi Shell, SSH, or the VMware Host Client.

- By default, you must include a mix of at least three from the following four character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash when you create a password.
- By default, password length is at least 7 characters and less than 40.
- Passwords must not contain a dictionary word or part of a dictionary word.
- Passwords must not contain the user name or parts of the user name.

Note: An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used. A dictionary word used inside a password reduces the overall password strength.

Example ESXi Passwords

The following password candidates illustrate potential passwords if the option is set as follows.

```
retry=3 min=disabled,disabled,disabled,7,7
```

With this setting, a user is prompted up to three times (retry=3) for a new password that is not sufficiently strong or if the password was not entered correctly twice. Passwords with one or two character classes and pass phrases are not allowed, because the first three items are disabled. Passwords from three- and four-character classes require seven characters. See the `pam_passwdqc` man page for details on other options, such as max, passphrase, and so on.

With these settings, the following passwords are allowed.

- xQaTEhb!: Contains eight characters from three character classes.

- xQaT3#A: Contains seven characters from four character classes.

The following password candidates do not meet requirements.

- Xqat3hi: Begins with an uppercase character, reducing the effective number of character classes to two. The minimum number of required character classes is three.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. The minimum number of required character classes is three.

ESXi Pass Phrase

Instead of a password, you can also use a pass phrase. However, pass phrases are disabled by default. You can change the default setting and other settings by using the Security.PasswordQualityControl advanced option from the vSphere Client.

For example, you can change the option to the following.

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows pass phrases of at least 16 characters and at least three words.

For legacy hosts, changing the `/etc/pam.d/passwd` file is still supported, but changing the file is deprecated for future releases. Use the Security.PasswordQualityControl advanced option instead.

Changing Default Password Restrictions

You can change the default restriction on passwords or pass phrases by using the Security.PasswordQualityControl advanced option for your ESXi host. See *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

You can change the default, for example, to require a minimum of 15 characters and a minimum number of four words (passphrase=4), as follows:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

See the man page for `pam_passwdqc` for details.

Note: Not all possible combinations of password options have been tested. Perform testing after you change the default password settings.

This example sets the password complexity requirement to require eight characters from four character classes that enforce a significant password difference, a remembered history of five passwords, and a 90 day rotation policy:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Set the Security.PasswordHistory option to 5 and the Security.PasswordMaxDays option to 90.

ESXi Account Lockout Behavior

Account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of five failed attempts is allowed before the account is locked. The account is unlocked after 15 minutes by default.

Configuring Login Behavior

You can configure the login behavior for your ESXi host with the following advanced options:

- Security.AccountLockFailures. Maximum number of failed login attempts before a user's account is locked. Zero deactivates account locking.
- Security.AccountUnlockTime. Number of seconds that a user is locked out.
- Security.PasswordHistory. Number of passwords to remember for each user. Zero deactivates password history.

See the *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

Cryptographic Key Generation

ESXi generates several asymmetric keys for normal operation. The Transport Layer Security (TLS) key secures communication with the ESXi host using the TLS protocol. The SSH key secures communication with the ESXi host using the SSH protocol.

Transport Layer Security Key

The Transport Layer Security (TLS) key secures communication with the host using the TLS protocol. Upon first boot, the ESXi host generates the TLS key as a 2048-bit RSA key. Currently, ESXi does not implement automatic generation of ECDSA keys for TLS. The TLS private key is not intended to be serviced by the administrator.

The TLS key resides at the following non-persistent location:

```
/etc/vmware/ssl/rui.key
```

The TLS public key (including intermediate certificate authorities) resides at the following non-persistent location as an X.509 v3 certificate :

```
/etc/vmware/ssl/rui.crt
```

When you use vCenter Server with your ESXi hosts, vCenter Server generates a CSR automatically, signs it using the VMware Certificate Authority (VMCA), and generates the certificate. When you add an ESXi host to vCenter Server, vCenter Server installs that resulting certificate on the ESXi host.

The default TLS certificate is self-signed, with a subjectAltName field matching the host name at installation. You can install a different certificate, for example, to make use of a different subjectAltName or to include a particular Certificate Authority (CA) in the verification chain. See Replacing ESXi SSL Certificates and Keys.

You can also use the VMware Host Client to replace the certificate. See *vSphere Single Host Management - VMware Host Client*.

SSH Key

The SSH key secures communication with the ESXi host using the SSH protocol. Upon first boot, the system generates a nistp256 ECDSA key, and the SSH keys as 2048-bit RSA keys. The SSH server is deactivated by default. SSH access is intended primarily for troubleshooting purposes. The SSH keys are not intended to be serviced by the administrator. Logging in through SSH requires administrative privileges equivalent to full host control. To enable SSH access, see Enable Access to the ESXi Shell.

The SSH public keys reside at the following location:

```
/etc/ssh/ssh_host_rsa_key.pub
```

```
/etc/ssh/ssh_host_ecdsa_key.pub
```

The SSH private keys reside at the following location:

```
/etc/ssh/ssh_host_rsa_key
```

```
/etc/ssh/ssh_host_ecdsa_key
```

TLS Cryptographic Key Establishment

Configuration of TLS cryptographic key establishment is governed by choice of TLS cipher suites, which select one of the RSA-based key transports (as specified in NIST Special Publication 800-56B) or ECC-based key agreements using ephemeral Ecliptic Curve Diffie Hellman (ECDH) (as specified in NIST Special Publication 800-56A).

SSH Cryptographic Key Establishment

Configuration of SSH cryptographic key establishment is governed by the SSHD configuration. ESXi provides a default configuration that permits RSA-based key transport (as specified in NIST Special Publication 800-56B), ephemeral Diffie Hellman (DH) (as specified in NIST Special Publication 800-56A) key agreement, and ephemeral Ecliptic Curve Diffie Hellman (ECHD) (as specified in NIST Special Publication 800-56A). The SSHD configuration is not intended to be serviced by the administrator.

SSH Security

ESXi Shell and SSH interfaces are disabled by default. Keep these interfaces disabled unless you are performing troubleshooting or support activities. For day-to-day activities, use the vSphere Client, where activity is subject to role-based access control and modern access control methods.

The SSH configuration in ESXi uses the following settings:

Version 1 SSH protocol disabled	VMware does not support Version 1 SSH protocol and uses Version 2 protocol exclusively. Version 2 eliminates certain security problems present in Version 1 and provides you with a safe way to communicate with the management interface.
Improved cipher strength	SSH supports only 256-bit and 128-bit AES ciphers for your connections.

These settings are designed to provide solid protection for the data you transmit to the management interface through SSH. You cannot change these settings.

ESXi SSH Keys

SSH keys can restrict, control, and secure access to an ESXi host. An SSH key can allow a trusted user or script to log in to a host without entering a password.

You can use HTTPS PUT to copy the SSK key to the host.

Instead of generating the keys externally and uploading them, you can create the keys on the ESXi host and download them. See the VMware knowledge base article at http://kb.vmware.com/kb/1002866.

Enabling SSH and adding SSH keys to the host has inherent risks. Weigh the potential risk of exposing a user name and password against the risk of intrusion by a user who has a trusted key.

Upload an SSH Key Using HTTPS PUT

You can use authorized keys to log in to a host with SSH. You can upload authorized keys with HTTPS PUT.

Authorized keys allow you to authenticate remote access to a host. When users or scripts try to access a host with SSH, the key provides authentication without a password. With authorized keys you can automate authentication, which is useful when you write scripts to perform routine tasks.
You can upload the following types of SSH keys to a host using HTTPS PUT:

- Authorized keys file for root user
- DSA key
- DSA public key
- RSA key
- RSA public key

Important: Do not modify the `/etc/ssh/sshd_config` file.

1. In your upload application, open the key file.
2. Publish the file to the following locations.

Type of key	Location
Authorized key files for the root user	`https://hostname_or_IP_address/host/ssh_root_authorized_keys` You must have full administrator privileges on the host to upload this file.
DSA keys	`https://hostname_or_IP_address/host/ssh_host_dsa_key`
DSA public keys	`https://hostname_or_IP_address/host/ssh_host_dsa_key_pub`
RSA keys	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
RSA public keys	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

PCI and PCIe Devices and ESXi

Using the VMware DirectPath I/O feature to pass through a PCI or PCIe device to a virtual machine results in a potential security vulnerability. The vulnerability can be triggered when buggy or malicious code, such as a device driver, is running in privileged mode in the guest OS. Industry-standard hardware and firmware do not currently have sufficient error containment support to protect ESXi hosts from the vulnerability.

Use PCI or PCIe passthrough to a virtual machine only if a trusted entity owns and administers the virtual machine. You must be sure that this entity does not to attempt to crash or exploit the host from the virtual machine.

Your host might be compromised in one of the following ways.

- The guest OS might generate an unrecoverable PCI or PCIe error. Such an error does not corrupt data, but can crash the ESXi host. Such errors might occur because of bugs or incompatibilities in the hardware devices that are being passed through. Other reasons for errors include problems with drivers in the guest OS.
- The guest OS might generate a Direct Memory Access (DMA) operation that causes an IOMMU page fault on the ESXi host. This operation might be the result of a DMA operation that targets an address outside the virtual machine memory. On some machines, host firmware configures IOMMU faults to report a fatal error through a non-maskable interrupt (NMI). This fatal error causes the ESXi host to crash. This problem might occur because of problems with the drivers in the guest OS.
- If the operating system on the ESXi host is not using interrupt remapping, the guest OS might inject a spurious interrupt into the ESXi host on any vector. ESXi currently uses interrupt remapping on Intel platforms where it is available. Interrupt mapping is part of the Intel VT-d feature set. ESXi does not use interrupt mapping on AMD platforms. A false interrupt can result in a crash of the ESXi host. Other ways to exploit these false interrupts might exist in theory.

Disable the Managed Object Browser

The managed object browser (MOB) provides a way to explore the VMkernel object model. However, attackers can use this interface to perform malicious configuration changes or actions because it is possible to change the host configuration by using the MOB. Use the MOB only for debugging, and ensure that it is disabled in production systems.

The MOB is disabled by default. However, for certain tasks, for example when extracting the old certificate from a system, you have to use the MOB. You can enable and disable the MOB as follows.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, click **Advanced System Settings**.
4. Check the value of **Config.HostAgent.plugins.solo.enableMob**, and click **Edit** to change it as appropriate.
   Do not use `vim-cmd` from the ESXi Shell.

ESXi Networking Security Recommendations

Isolation of network traffic is essential to a secure ESXi environment. Different networks require a different access and level of isolation.

Your ESXi host uses several networks. Use appropriate security measures for each network, and isolate traffic for specific applications and functions. For example, ensure that VMware vSphere® vMotion® traffic does not travel over networks where virtual machines are located. Isolation prevents snooping. Having separate networks is also recommended for performance reasons.

- vSphere infrastructure networks are used for features such as vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN, and storage. Isolate these networks for their specific functions. It is often not necessary to route these networks outside a single physical server rack.
- A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from other traffic. This network should be accessible only by system, network, and security administrators. Use jump box or virtual private network (VPN) to secure access to the management network. Strictly control access within this network.
- Virtual machine traffic can flow over one or many networks. You can enhance the isolation of virtual machines by using virtual firewall solutions that set firewall rules at the virtual network controller. These settings travel with a virtual machine as it migrates from host to host within your vSphere environment.

Modifying ESXi Web Proxy Settings

When you modify Web proxy settings, you have several encryption and user security guidelines to consider.

Note: Restart the host process after making any changes to host directories or authentication mechanisms.

- Do not set up certificates that use a password or pass phrases. ESXi does not support Web proxies that use passwords or pass phrases, also known as encrypted keys. If you set up a Web proxy that requires a password or pass phrase, ESXi processes cannot start correctly.
- To support encryption for user names, passwords, and packets, SSL is enabled by default for vSphere Web Services SDK connections. If you want to configure these connections so that they do not encrypt transmissions, disable SSL for your vSphere Web Services SDK connection by switching the connection from HTTPS to HTTP.
  Consider disabling SSL only if you created a fully trusted environment for these clients, where firewalls are in place and transmissions to and from the host are fully isolated. Disabling SSL can improve performance, because you avoid the overhead required to perform encryption.
- To protect against misuse of ESXi services, most internal ESXi services are accessible only through port 443, the port used for HTTPS transmission. Port 443 acts as a reverse proxy for ESXi. You can see a list of services on

ESXi through an HTTP welcome page, but you cannot directly access the Storage Adapters services without proper authorization.

You can change this configuration so that individual services are directly accessible through HTTP connections. Do not make this change unless you are using ESXi in a fully trusted environment.

- When you upgrade your environment, the certificate remains in place.

vSphere Auto Deploy Security Considerations

When you use vSphere Auto Deploy, mind networking security, boot image security, and potential password exposure to protect your environment.

Networking Security

Secure your network just as you secure the network for any other PXE-based deployment method. vSphere Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or of the Auto Deploy server is not checked during a PXE boot.

You can greatly reduce the security risk of Auto Deploy by completely isolating the network where Auto Deploy is used.

Boot Image and Host Profile Security

The boot image that the vSphere Auto Deploy server downloads to a machine can have the following components.

- The VIB packages that the image profile consists of are always included in the boot image.
- The host profile and host customization are included in the boot image if Auto Deploy rules are set up to provision the host with a host profile or host customization.
  - The administrator (root) password and user passwords that are included with host profile and host customization are hashed with SHA-512.
  - Any other passwords associated with profiles are in the clear. If you set up Active Directory by using host profiles, the passwords are not protected.

    Use the vSphere Authentication Proxy to avoid exposing the Active Directory passwords. If you set up Active Directory using host profiles, the passwords are not protected.
- The host's public and private SSL key and certificate are included in the boot image.

Control Access for CIM-Based Hardware Monitoring Tools

The Common Information Model (CIM) system provides an interface that enables hardware-level management from remote applications using a set of standard APIs. To ensure that the CIM interface is secure, provide only the minimum access necessary to these remote applications. If you provision a remote application with a root or Administrator account, and if the application is compromised, the virtual environment can be compromised.

CIM is an open standard that defines a framework for agent-less, standards-based monitoring of hardware resources for ESXi hosts. This framework consists of a CIM object manager, often called a CIM broker, and a set of CIM providers.

CIM providers support management access to device drivers and underlying hardware. Hardware vendors, including server manufacturers and hardware device vendors, can write providers that monitor and manage their devices. VMware writes providers that monitor server hardware, ESXi storage infrastructure, and virtualization-specific resources. These providers run inside the ESXi host and are lightweight and focused on specific management tasks. The CIM broker takes information from all CIM providers and presents it to the outside world using standard APIs. The most common API is WS-MAN.

Do not provide root credentials to remote applications that access the CIM interface. Instead, create a less-privileged vSphere user account for these applications and use the VIM API ticket function to issue a sessionId (called a "ticket") to this less-privileged user account to authenticate to CIM. If the account has been granted permission to obtain CIM tickets,

the VIM API can then supply the ticket to CIM. These tickets are then supplied as both the user ID and password to any CIM-XML API call. See the `AcquireCimServicesTicket()` method for more information.

The CIM service starts when you install a third-party CIM VIB, for example, when you run the `esxcli software vib install -n` *`VIBname`* command.

If you must enable the CIM service manually, run the following command:

```
esxcli system wbem set -e true
```

If necessary, you can disable wsman (WSManagement Service) so that only the CIM service is running:

```
esxcli system wbem set -W false
```

To confirm that wsman is disabled, run the following command:

```
esxcli system wbem get
…
WSManagement PID: 0
WSManagement Service: false
```

For more information about ESXCLI commands, see *ESXCLI Documentation*. For more information about enabling the CIM service, see the VMware knowledge base article at https://kb.vmware.com/kb/1025757.

1. Create a non-root vSphere user account for CIM applications.

   See the topic on adding vCenter Single Sign-On users in *vSphere Authentication*. The required vSphere privilege for the user account is **Host.CIM** > **Interaction**.

2. Use the vSphere API SDK of your choice to authenticate the user account to vCenter Server. Then call `AcquireCimServicesTicket()` to return a ticket to authenticate with ESXi as an administrator-level account using CIM-XML port 5989 or WS-Man port 433 APIs.

   See *vSphere Web Services API Reference* for more information.

3. Renew the ticket every two minutes as needed.

Certificate Management for ESXi Hosts

The VMware Certificate Authority (VMCA) provisions each new ESXi host with a signed certificate that has VMCA as the root certificate authority by default. Provisioning happens when the host is added to vCenter Server explicitly or as part of installation or upgrade to ESXi 6.0 or later.

You can view and manage ESXi certificates from the vSphere Client and by using the `vim.CertificateManager` API in the vSphere Web Services SDK. You cannot view or manage ESXi certificates by using certificate management CLIs that are available for managing vCenter Server certificates.

Certificates in vSphere 6.0 and Later

When ESXi and vCenter Server communicate, they use TLS for almost all management traffic.

In vSphere 6.0 and later, vCenter Server supports the following certificate modes for ESXi hosts.

Table 238: Certificate Modes for ESXi Hosts

Certificate Mode	Description
VMware Certificate Authority (default)	Use this mode if VMCA provisions all ESXi hosts, either as the top-level CA or as an intermediate CA. By default, VMCA provisions ESXi hosts with certificates.

Certificate Mode	Description
	In this mode, you can refresh and renew certificates from the vSphere Client.
Custom Certificate Authority	Use this mode if you want to use only custom certificates that are signed by a third-party or enterprise CA. In this mode, you are responsible for managing the certificates. You cannot refresh and renew certificates from the vSphere Client. **Note:** Unless you change the certificate mode to Custom Certificate Authority, VMCA might replace custom certificates, for example, when you select **Renew** in the vSphere Client.
Thumbprint Mode	vSphere 5.5 used thumbprint mode, and this mode is still available as a fallback option for vSphere 6.x. In this mode, vCenter Server checks that the certificate is formatted correctly, but does not check the validity of the certificate. Even expired certificates are accepted. Do not use this mode unless you encounter problems that you cannot resolve with one of the other two modes. Some vCenter 6.x and later services might not work correctly in thumbprint mode.

Certificate Expiration

You can view information about certificate expiration for certificates that are signed by VMCA or a third-party CA in the vSphere Client. You can view the information for all hosts that are managed by a vCenter Server or for individual hosts. A yellow alarm is raised if the certificate is in the **Expiring Shortly** state (less than eight months). A red alarm is raised if the certificate is in the **Expiration Imminent** state (less than two months).

ESXi Provisioning and VMCA

When you boot an ESXi host from installation media, the host initially has an autogenerated certificate. When the host is added to the vCenter Server system, it is provisioned with a certificate that is signed by VMCA as the root CA.

The process is similar for hosts that are provisioned with Auto Deploy. However, because those hosts do not store any state, the signed certificate is stored by the Auto Deploy server in its local certificate store. The certificate is reused during subsequent boots of the ESXi hosts. An Auto Deploy server is part of any embedded deployment or vCenter Server system.

If VMCA is not available when an Auto Deploy host boots the first time, the host first attempts to connect. If the host cannot connect, it cycles through shutdown and reboot until VMCA becomes available and the host can be provisioned with a signed certificate.

Required Privileges for ESXi Certificate Management

For certificate management for ESXi hosts, you must have the **Certificates** > **Manage Certificates** privilege. You can set that privilege from the vSphere Client.

Host Name and IP Address Changes

A host name or IP address change might affect whether vCenter Server considers a host certificate valid. How you added the host to vCenter Server affects whether manual intervention is necessary. Manual intervention means that you either reconnect the host, or you remove the host from vCenter Server and add it back.

Table 239: When Host Name or IP Address Changes Require Manual Intervention

Host added to vCenter Server using...	Host name changes	IP address changes
Host name	vCenter Server connectivity problem. Manual intervention required.	No intervention required.
IP address	No intervention required.	vCenter Server connectivity problem. Manual intervention required.

Host Upgrades and Certificates

If you upgrade an ESXi host to ESXi 6.5 or later, the upgrade process replaces the self-signed (thumbprint) certificates with VMCA-signed certificates. If the ESXi host uses custom certificates, the upgrade process retains those certificates even if those certificates are expired or invalid.

The recommended upgrade workflow depends on the current certificates.

Host Provisioned with Thumbprint Certificates

If your host is currently using thumbprint certificates, it is automatically assigned VMCA certificates as part of the upgrade process.

Note: You cannot provision legacy hosts with VMCA certificates. You must upgrade those hosts to ESXi 6.5 or later.

Host Provisioned with Custom Certificates

If your host is provisioned with custom certificates, usually third-party CA-signed certificates, those certificates remain in place during upgrade. Change the certificate mode to **Custom** to ensure that the certificates are not replaced accidentally during a certificate refresh later.

Note: If your environment is in VMCA mode, and you refresh the certificates from the vSphere Client, any existing certificates are replaced with certificates that are signed by VMCA.

Going forward, vCenter Server monitors the certificates and displays information, for example, about certificate expiration, in the vSphere Client.

Hosts Provisioned with Auto Deploy

Hosts that are being provisioned by Auto Deploy are always assigned new certificates when they are first booted with ESXi 6.5 or later software. When you upgrade a host that is provisioned by Auto Deploy, the Auto Deploy server generates a certificate signing request (CSR) for the host and submits it to VMCA. VMCA stores the signed certificate for the host. When the Auto Deploy server provisions the host, it retrieves the certificate from VMCA and includes it as part of the provisioning process.

You can use Auto Deploy with custom certificates.

Certificate Mode Switch Workflows

Starting with vSphere 6.0, ESXi hosts are provisioned with certificates by VMCA by default. You can instead use custom certificate mode or, for debugging purposes, the legacy thumbprint mode. In most cases, mode switches are disruptive and not necessary. If you do require a mode switch, review the potential impact before you start.

In vSphere 6.0 and later, vCenter Server supports the following certificate modes for ESXi hosts.

Certificate Mode	Description
VMware Certificate Authority (default)	By default, the VMware Certificate Authority is used as the CA for ESXi host certificates. VMCA is the root CA by default, but it can be set up as the intermediary CA to another CA. In this mode, users can manage certificates from the vSphere Client. Also used if VMCA is a subordinate certificate.
Custom Certificate Authority	Some customers might prefer to manage their own external certificate authority. In this mode, customers are responsible for managing the certificates and cannot manage them from the vSphere Client.
Thumbprint Mode	vSphere 5.5 used thumbprint mode, and this mode is still available as a fallback option for vSphere 6.0. Do not use this mode unless you encounter problems with one of the other two modes that you cannot resolve. Some vCenter 6.0 and later services might not work correctly in thumbprint mode.

Using Custom ESXi Certificates

If your company policy requires that you use a different root CA than VMCA, you can switch the certificate mode in your environment after careful planning. The workflow is as follows.

1. Obtain the certificates that you want to use.
2. Place the host or hosts into maintenance mode and disconnect them from vCenter Server.
3. Add the custom CA's root certificate to VECS.
4. Deploy the custom CA certificates to each host and restart services on that host.
5. Switch to Custom CA mode. See Change the Certificate Mode.
6. Connect the host or hosts to the vCenter Server system.

Switching from Custom CA Mode to VMCA Mode

If you are using custom CA mode and decide that using VMCA works better in your environment, you can perform the mode switch after careful planning. The workflow is as follows.

1. Remove all hosts from the vCenter Server system.
2. On the vCenter Server system, remove the third-party CA's root certificate from VECS.
3. Switch to VMCA mode. See Change the Certificate Mode.
4. Add the hosts to the vCenter Server system.

Note: Any other workflow for this mode switch might result in unpredictable behavior.

Retaining Thumbprint Mode Certificates During Upgrade

The switch from VMCA mode to thumbprint mode might be necessary if you encounter problems with the VMCA certificates. In thumbprint mode, the vCenter Server system checks only whether a certificate exists and is formatted correctly, and does not check whether the certificate is valid. See Change the Certificate Mode for instructions.

Switching from Thumbprint Mode to VMCA Mode

If you use thumbprint mode and you want to start using VMCA-signed certificates, the switch requires some planning. The workflow is as follows.

1. Remove all hosts from the vCenter Server system.
2. Switch to VMCA certificate mode. See Change the Certificate Mode.

3. Add the hosts to the vCenter Server system.

Note: Any other workflow for this mode switch might result in unpredictable behavior.

Switching from Custom CA Mode to Thumbprint Mode

If you are encountering problems with your custom CA, consider switching to thumbprint mode temporarily. The switch works seamlessly if you follow the instructions in Change the Certificate Mode. After the mode switch, the vCenter Server system checks only the format of the certificate and no longer checks the validity of the certificate itself.

Switching from Thumbprint Mode to Custom CA Mode

If you set your environment to thumbprint mode during troubleshooting, and you want to start using custom CA mode, you must first generate the required certificates. The workflow is as follows.

1. Remove all hosts from the vCenter Server system.
2. Add the custom CA root certificate to TRUSTED_ROOTS store on VECS on the vCenter Server system. See Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates).
3. For each ESXi host:
   a. Deploy the custom CA certificate and key.
   b. Restart services on the host.
4. Switch to custom mode. See Change the Certificate Mode.
5. Add the hosts to the vCenter Server system.

ESXi Certificate Default Settings

When a host is added to a vCenter Server system, vCenter Server sends a Certificate Signing Request (CSR) for the host to VMCA. Most of the default values are well suited for many situations, but company-specific information can be changed.

You can change many of the default settings using the vSphere Client. Consider changing the organization, and location information. See Change Certificate Default Settings.

Table 240: ESXi CSR Settings

Parameter	Default Value	Advanced Option
Key Size	2048	N.A.
Key Algorithm	RSA	N.A.
Certificate Signature Algorithm	sha256WithRSAEncryption	N.A.
Common Name	Name of the host if the host was added to vCenter Server by host name. IP address of the host if the host was added to vCenter Server by IP address.	N.A.
Country	US	vpxd.certmgmt.certs.cn.country
Email address	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Locality (City)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Organization Unit Name	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Organization Name	VMware	vpxd.certmgmt.certs.cn.organizationName

Parameter	Default Value	Advanced Option
State or province	California	vpxd.certmgmt.certs.cn.state
Number of days the certificate is valid.	1825	vpxd.certmgmt.certs.daysValid
Hard threshold for the certificate expiration. vCenter Server raises a red alarm when this threshold is reached.	30 days	vpxd.certmgmt.certs.hardThreshold
Poll interval for vCenter Server certificate validity checks.	5 days	vpxd.certmgmt.certs.pollIntervalDays
Soft threshold for the certificate expiration. vCenter Server raises an event when this threshold is reached.	240 days	vpxd.certmgmt.certs.softThreshold
Mode that vCenter Server users to determine whether existing certificates are replaced. Change this mode to retain custom certificates during upgrade. See Host Upgrades and Certificates.	vmca You can also specify thumbprint or custom. See Change the Certificate Mode.	vpxd.certmgmt.mode

Change Certificate Default Settings

When a host is added to a vCenter Server system, vCenter Server sends a Certificate Signing Request (CSR) for the host to VMCA. You can change some of the default settings in the CSR using the vCenter Server Advanced Settings in the vSphere Client.

See ESXi Certificate Default Settings for a list of default settings. Some of the defaults cannot be changed.

1. In the vSphere Client, select the vCenter Server system that manages the hosts.
2. Click **Configure**, and click **Advanced Settings**.
3. Click **Edit Settings**.
4. Click the **Filter** icon in the Name column, and in the Filter box, enter `vpxd.certmgmt` to display only certificate management parameters.
5. Change the value of the existing parameters to follow your company policy and click **Save**.

   The next time you add a host to vCenter Server, the new settings are used in the CSR that vCenter Server sends to VMCA and in the certificate that is assigned to the host.

Changes to certificate metadata only affect new certificates. If you want to change the certificates of hosts that are already managed by the vCenter Server system, you can disconnect and reconnect the hosts or renew the certificates.

View Certificate Expiration Information for Multiple ESXi Hosts

If you are using ESXi 6.0 and later, you can view the certificate status of all hosts that are managed by your vCenter Server system. The display allows you to determine whether any of the certificates expire soon.

You can view certificate status information for hosts that are using VMCA mode and for hosts that are using custom mode in the vSphere Client. You cannot view certificate status information for hosts in thumbprint mode.

1. Log in to the vCenter Server by using the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Select **Hosts & Clusters** > **Hosts**.
   By default, the Hosts display does not include the certificate status.
4. To show or hide columns, click the three-bar **Column Selector** in the lower left corner.
5. Select the **Certificate Valid To** check box, and scroll to the right if necessary to view the added column.
   The certificate information displays when the certificate expires.
   If a host is added to vCenter Server or reconnected after a disconnect, vCenter Server renews the certificate if the status is Expired, Expiring, Expiring shortly, or Expiration imminent. The status is Expiring if the certificate is valid for less than eight months, Expiring shortly if the certificate is valid for less than two months, and Expiration imminent if the certificate is valid for less than one month.
6. Optional: Deselect other columns to make it easier to see what you are interested in.

Renew the certificates that are about to expire. See Renew or Refresh ESXi Certificates.

View Certificate Details for a Single ESXi Host

For ESXi 6.0 and later hosts that are in VMCA mode or custom mode, you can view certificate details from the vSphere Client. The information about the certificate can be helpful for debugging.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under **System**, click **Certificate**.
   You can examine the following information. This information is available only in the single-host view.

Field	Description
Subject	The subject used during certificate generation.
Issuer	The issuer of the certificate.
Valid From	Date on which the certificate was generated.
Valid To	Date on which the certificate expires.
Status	Status of the certificate, one of the following. **Good** Normal operation. **Expiring** Certificate expires soon. **Expiring shortly** Certificate is eight months or less away from expiration (Default). **Expiration imminent** Certificate is two months or less away from expiration (Default). **Expired** Certificate is not valid because it expired.

Renew or Refresh ESXi Certificates

If VMCA assigns certificates to your ESXi hosts (6.0 and later), you can renew those certificates from the vSphere Client. You can also refresh all certificates from the TRUSTED_ROOTS store associated with vCenter Server.

Verify the following:

- The ESXi hosts are connected to the vCenter Server system.
- There is proper time synchronization between the vCenter Server system and the ESXi hosts.
- DNS resolution works between the vCenter Server system and the ESXi hosts.
- The vCenter Server system's MACHINE_SSL_CERT and Trusted_Root certificates are valid and have not expired. See the VMware knowledge base article at https://kb.vmware.com/s/article/2111411.
- The ESXi hosts are not in maintenance mode.

You can renew your certificates when they are about to expire, or if you want to provision the host with a new certificate for other reasons. If you do not renew the certificate before it expires, disconnecting the host and reconnecting it causes vCenter Server to renew the certificate. The act of re-adding the host to vCenter Server reestablishes trust, and enables vCenter Server to unconditionally issue the renewed certificate.

By default, vCenter Server renews the certificates of a host with status Expired, Expiration imminent, or Expiring shortly, each time the host is added to the inventory, or reconnected.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under **System**, click **Certificate**.

   You can view detailed information about the selected host's certificate.
4. Click **Renew** or **Refresh CA Certificates**.

Option	Description
Renew	Retrieves a fresh signed certificate for the host from VMCA.
Refresh CA Certificates	Pushes all certificates in the TRUSTED_ROOTS store in the vCenter Server VECS store to the host.

5. Click **Yes** to confirm.

Change the Certificate Mode

Use VMware Certificate Authority (VMCA) to provision certificates of the ESXi hosts in your environment unless corporate policy requires that you use custom certificates. To use custom certificates with a different root CA, you can edit the vCenter Servervpxd.certmgmt.mode advanced option. After the change, the hosts are no longer automatically provisioned

with VMCA certificates when you refresh the certificates. You are responsible for the certificate management in your environment.

You can use the vCenter Server advanced settings to change to thumbprint mode or to custom CA mode. Use thumbprint mode only as a fallback option.

1. In the vSphere Client, select the vCenter Server system that manages the hosts.
2. Click **Configure**, and under Settings, click **Advanced Settings**.
3. Click **Edit Settings**.
4. Click the **Filter** icon in the Name column, and in the Filter box, enter `vpxd.certmgmt` to display only certificate management parameters.
5. Change the value of vpxd.certmgmt.mode to **custom** if you intend to manage your own certificates, and to **thumbprint** if you temporarily want to use thumbprint mode, and click **Save**.
6. Restart the vCenter Server service.

   See the *vCenter Server Configuration* documentation for information about restarting services.

Replacing ESXi SSL Certificates and Keys

Your company's security policy might require that you replace the default ESXi SSL certificate with a third-party CA-signed certificate on each host.

By default, vSphere components use the VMCA-signed certificate and key that are created during installation. If you accidentally delete the VMCA-signed certificate, remove the host from its vCenter Server system, and add it back. When you add the host, vCenter Server requests a new certificate from VMCA and provisions the host with it.

Replace VMCA-signed certificates with certificates from a trusted CA, either a commercial CA or an organizational CA, if your company policy requires it.

The default certificates are in the same location as the vSphere 5.5 certificates. You can replace the default certificates with trusted certificates in various ways.

Note: You can also use the `vim.CertificateManager` and `vim.host.CertificateManager` managed objects in the vSphere Web Services SDK. See the vSphere Web Services SDK documentation.

After you replace the certificate, you have to update the TRUSTED_ROOTS store in VECS on the vCenter Server system that manages the host to ensure that the vCenter Server and the ESXi host have a trust relationship.

For detailed instructions about using CA-signed certificates for ESXi hosts, see Certificate Mode Switch Workflows.

Note: If you are replacing SSL certificates on an ESXi host that is part of a vSAN cluster, follow the steps that are in the VMware knowledge base article at https://kb.vmware.com/s/article/56441.

Requirements for ESXi Certificate Signing Requests

If you want to use an enterprise or third-party CA-signed certificate, or a subordinate CA-signed certificate, you have to send a Certificate Signing Request (CSR) to the CA.

Use a CSR with these characteristics:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
- x509 version 3
- For root certificates, the CA extension must be set to true, and the cert sign must be in the list of requirements.

- SubjectAltName must contain DNS Name=<machine_FQDN>.
- CRT format
- Contains the following Key Usages: Digital Signature, Key Encipherment
- Start time of one day before the current time.
- CN (and SubjectAltName) set to the host name (or IP address) that the ESXi host has in the vCenter Server inventory.

vSphere does not support the following certificates.

- Certificates with wildcards.
- The algorithms md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1, and sha1WithRSAEncryption are not supported.

For information about generating the CSR, see the VMware knowledge base article at https://kb.vmware.com/s/article/2113926.

Related Links

Replace the Default Certificate and Key from theESXi Shell on page 2734
You can replace the default VMCA-signedESXi certificates from theESXi Shell.

Replace a Default Certificate Using HTTPS PUT on page 2735
You can use third-party applications to upload certificates and key. Applications that support HTTPS PUT operations work with the HTTPS interface that is included withESXi.

Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates) on page 2736
If you set up your ESXi hosts to use custom certificates, you must update the `TRUSTED_ROOTS` store on the vCenter Server system that manages the hosts.

Replace the Default Certificate and Key from theESXi Shell

You can replace the default VMCA-signedESXi certificates from theESXi Shell.

- If you want to use third-party CA-signed certificates, generate the certificate request, send it to the certificate authority, and store the certificates on each ESXi host.
- If necessary, enable the ESXi Shell or enable SSH traffic from the vSphere Client.
- All file transfers and other communications occur over a secure HTTPS session. The user who is used to authenticate the session must have the privilege **Host** > **Config** > **AdvancedConfig** on the host.

1. Log in to theESXi Shell, either directly from the DCUI or from an SSH client, as a user with administrator privileges.
2. In the directory `/etc/vmware/ssl`, rename the existing certificates using the following commands.

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3. Copy the certificates that you want to use to `/etc/vmware/ssl`.
4. Rename the new certificate and key to `rui.crt` and `rui.key`.
5. Restart the host after you install the new certificate.

   Alternatively, you can put the host into maintenance mode, install the new certificate, use the Direct Console User Interface (DCUI) to restart the management agents, and set the host to exit maintenance mode.

Update the TRUSTED_ROOTS store. See Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates).

Related Links

Requirements for ESXi Certificate Signing Requests on page 2733
If you want to use an enterprise or third-party CA-signed certificate, or a subordinate CA-signed certificate, you have to send a Certificate Signing Request (CSR) to the CA.

Replace a Default Certificate Using HTTPS PUT on page 2735
You can use third-party applications to upload certificates and key. Applications that support HTTPS PUT operations work with the HTTPS interface that is included withESXi.

Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates) on page 2736
If you set up your ESXi hosts to use custom certificates, you must update the `TRUSTED_ROOTS` store on the vCenter Server system that manages the hosts.

Replace a Default Certificate Using HTTPS PUT

You can use third-party applications to upload certificates and key. Applications that support HTTPS PUT operations work with the HTTPS interface that is included withESXi.

- If you want to use third-party CA-signed certificates, generate the certificate request, send it to the certificate authority, and store the certificates on each ESXi host.
- If necessary, enable the ESXi Shell or enable SSH traffic from the vSphere Client.
- All file transfers and other communications occur over a secure HTTPS session. The user who is used to authenticate the session must have the privilege **Host** > **Config** > **AdvancedConfig** on the host.

1. Back up the existing certificates.
2. Set up basic access authentication, in which you supply a Base64 encoded username and password, separated with a single colon (:). For more information, see https://en.wikipedia.org/wiki/Basic_access_authentication.
3. In your upload application, process each file as follows:
   a) Open the file.
   b) Publish the file to one of these locations.

Option	Description
Certificates	`https://hostname/host/ssl_cert`
Keys	`https://hostname/host/ssl_key`

   The `/host/ssl_cert` and the `host/ssl_key` locations link to the certificate files in `/etc/vmware/ssl`.
4. Restart the host.

   Alternatively, you can put the host into maintenance mode, install the new certificate, use the Direct Console User Interface (DCUI) to restart the management agents, and set the host to exit maintenance mode.

Update thevCenter Server TRUSTED_ROOTS store. See Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates).

Related Links

Requirements for ESXi Certificate Signing Requests on page 2733
If you want to use an enterprise or third-party CA-signed certificate, or a subordinate CA-signed certificate, you have to send a Certificate Signing Request (CSR) to the CA.

Replace the Default Certificate and Key from theESXi Shell on page 2734
You can replace the default VMCA-signedESXi certificates from theESXi Shell.

Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates) on page 2736
If you set up your ESXi hosts to use custom certificates, you must update the `TRUSTED_ROOTS` store on the vCenter Server system that manages the hosts.

Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates)

If you set up your ESXi hosts to use custom certificates, you must update the `TRUSTED_ROOTS` store on the vCenter Server system that manages the hosts.

Replace the certificates on each host with custom certificates.

Note: This step is not required if the vCenter Server system is also running with custom certificates issued by the same CA as those installed on the ESXi hosts.

1. Log in to the vCenter Server shell of the vCenter Server system that manages the ESXi hosts.
2. To add the new certificates to the `TRUSTED_ROOTS` store, run `dir-cli`, for example:

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_RootCA
   ```

3. When prompted, provide the Single Sign-On Administrator credentials.
4. If your custom certificates are issued by an intermediate CA, you must also add the intermediate CA to the `TRUSTED_ROOTS` store on the vCenter Server, for example:

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_intermediateCA
   ```

Set certificate mode to Custom. If the certificate mode is VMCA, the default, and you perform a certificate refresh, your custom certificates are replaced with VMCA-signed certificates. See Change the Certificate Mode.

Related Links

Requirements for ESXi Certificate Signing Requests on page 2733
If you want to use an enterprise or third-party CA-signed certificate, or a subordinate CA-signed certificate, you have to send a Certificate Signing Request (CSR) to the CA.

Replace the Default Certificate and Key from theESXi Shell on page 2734
You can replace the default VMCA-signedESXi certificates from theESXi Shell.

Replace a Default Certificate Using HTTPS PUT on page 2735
You can use third-party applications to upload certificates and key. Applications that support HTTPS PUT operations work with the HTTPS interface that is included withESXi.

Use Custom Certificates with Auto Deploy

By default, the Auto Deploy server provisions each host with certificates that are signed by VMCA. You can set up the Auto Deploy server to provision all hosts with custom certificates that are not signed by VMCA. In that scenario, the Auto Deploy server becomes a subordinate certificate authority of your third-party CA.

- Request a certificate from your CA. The certificate must meet these requirements.
  - Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
  - PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
  - x509 version 3
  - For root certificates, the CA extension must be set to true, and the cert sign must be in the list of requirements.
  - SubjectAltName must contain DNS Name=<machine_FQDN>.
  - CRT format
  - Contains the following Key Usages: Digital Signature, Key Encipherment
  - Start time of one day before the current time.
  - CN (and SubjectAltName) set to the host name (or IP address) that the ESXi host has in the vCenter Server inventory.

- Name the certificate and the key files `rbd-ca.crt` and `rbd-ca.key`.

1. Back up the default ESXi certificates.
   The certificates are in the `/etc/vmware-rbd/ssl/` directory.
2. Stop the vSphere Authentication Proxy service.

Tool	Steps
vCenter Server Management Interface	1. In a Web browser, go to the vCenter Server Management Interface, https://*vcenter-IP-address-or-FQDN*:5480. 2. Log in as root. The default root password is the password that you set while deploying the vCenter Server. 3. Click **Services**, and click the **VMware vSphere Authentication Proxy service**. 4. Click **Stop**.
CLI	`service-control --stop vmcam`

3. On the system where the Auto Deploy service runs, replace `rbd-ca.crt` and `rbd-ca.key` in `/etc/vmware-rbd/ssl/` with your custom certificate and key files.
4. On the system where the Auto Deploy service runs, run the following command to update the TRUSTED_ROOTS store inside the VECS to use your new certificates.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt
/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh
```

5. Create a `castore.pem` file that contains what is in the TRUSTED_ROOTS store and place the file in the `/etc/vmware-rbd/ssl/` directory.
   In custom mode, you are responsible for maintaining this file.
6. Change the ESXi certificate mode for the vCenter Server system to `custom`.
   See Change the Certificate Mode.
7. Restart the vCenter Server service and start the Auto Deploy service.

The next time you provision a host that is set up to use Auto Deploy, the Auto Deploy server generates a certificate. The Auto Deploy server uses the root certificate that you added to the TRUSTED_ROOTS store.

Note: If you encounter problems with Auto Deploy after certificate replacement, see the VMware knowledge base article at http://kb.vmware.com/kb/2000988.

Restore ESXi Certificate and Key Files

When you replace a certificate on an ESXi host by using the vSphere Web Services SDK, the previous certificate and key are appended to a `.bak` file. You can restore previous certificates by moving the information in the `.bak` file to the current certificate and key files.

The host certificate and key are located in `/etc/vmware/ssl/rui.crt` and `/etc/vmware/ssl/rui.key`. When you replace a host certificate and key by using the vSphere Web Services SDK `vim.CertificateManager` managed object, the previous key and certificate are appended to the file `/etc/vmware/ssl/rui.bak`.

Note: If you replace the certificate by using HTTP PUT or from the ESXi Shell, the existing certificates are not appended to the `.bak` file.

1. On the ESXi host, locate the file `/etc/vmware/ssl/rui.bak`.
   The file has the following format.

```
#
```

```
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

2. Copy the text starting with `-----BEGIN PRIVATE KEY-----` and ending with `-----END PRIVATE KEY-----` into the `/etc/vmware/ssl/rui.key` file.

   Include `-----BEGIN PRIVATE KEY-----` and `-----END PRIVATE KEY-----` .

3. Copy the text between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` into the `/etc/vmware/ssl/rui.crt` file.

   Include `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` .

4. Restart the ESXi host.

   Alternatively, you can put the host into maintenance mode and use the Direct Console User Interface (DCUI) to restart the management agents, and set the host to exit maintenance mode.

Customizing Hosts with the Security Profile

You can customize many of the essential security settings for your host through the Security Profile, Services, and Firewall panels available in the vSphere Client. The Security Profile is especially useful for single host management. If you are managing multiple hosts, consider using one of the CLIs or SDKs and automating the customization.

ESXi Firewall Configuration

ESXi includes a firewall that is enabled by default.

At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the security profile of the host.

As you open ports on the firewall, consider that unrestricted access to services running on an ESXi host can expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to enable access only from authorized networks.

Note: The firewall also allows Internet Control Message Protocol (ICMP) pings and communication with DHCP and DNS (UDP only) clients.

You can manage ESXi firewall ports as follows:

- Use **Configure** > **Firewall** for each host in the vSphere Client. See Manage ESXi Firewall Settings.
- Use ESXCLI commands from the command line or in scripts. See ESXi ESXCLI Firewall Commands.
- Use a custom VIB if the port you want to open is not included in the security profile.

  To install the custom VIB, you have to change the acceptance level of the ESXi host to CommunitySupported.

  Note: If you engage VMware Technical Support to investigate a problem on an ESXi host with a CommunitySupported VIB installed, VMware Support can request you to uninstall this VIB. Such a request is a troubleshooting step to determine if that VIB is related to the problem being investigated.

The behavior of the NFS Client rule set (`nfsClient`) is different from other rule sets. When the NFS Client rule set is enabled, all outbound TCP ports are open for the destination hosts in the list of allowed IP addresses. See NFS Client Firewall Behavior for more information.

Manage ESXi Firewall Settings

You can configure incoming and outgoing firewall connections for a service or a management agent from the vSphere Client or at the command line.

This task describes how to use the vSphere Client to configure ESXi firewall settings. You can use the ESXi Shell or ESXCLI commands to configure ESXi at the command line to automate the firewall configuration. See *Getting Started with ESXCLI* for an introduction, and *ESXCLI Concepts and Examples* for examples of using ESXCLI to manipulate firewalls and firewall rules.

Note: If different services have overlapping port rules, enabling one service might implicitly enable other services. You can specify which IP addresses are allowed to access each service on the host to avoid this problem.

1. Log in to the vCenter Server by using the vSphere Client.
2. Browse to the host in the inventory.
3. Click **Configure**, then click **Firewall** under **System**.
   You can toggle between incoming and outgoing connections by clicking **Incoming** and **Outgoing**.
4. In the Firewall section, click **Edit**.
5. Select from one of the three service groups, **Ungrouped**, **Secure Shell**, and **Simple Network Management Protocol**.
6. Select the rule sets to enable, or deselect the rule sets to disable.
7. For some services, you can also manage service details by navigating to **Configure** > **Services** under System.
   For more information about starting, stopping, and restarting services, see Enable or Disable a Service.
8. For some services, you can explicitly specify IP addresses from which connections are allowed.
   See Add Allowed IP Addresses for an ESXi Host.
9. Click **OK**.

Add Allowed IP Addresses for an ESXi Host

By default, the firewall for each service allows access to all IP addresses. To restrict traffic, change each service to allow traffic only from your management subnet. You can also deselect some services if your environment does not use them.

To update the Allowed IP list for a service you can use the vSphere Client, ESXCLI, or PowerCLI. By default, all IP addresses are allowed for a service. This task describes how to use the vSphere Client. See the topic on managing the firewall in *ESXCLI Concepts and Examples* at https://code.vmware.com/ for instructions on using ESXCLI.

1. Log in to the vCenter Server by using the vSphere Client.
2. Browse to the ESXi host.
3. Click **Configure**, then click **Firewall** under **System**.
   You can toggle between incoming and outgoing connections by clicking **Incoming** and **Outgoing**.

4. In the Firewall section, click **Edit**.
5. Select from one of the three service groups, **Ungrouped**, **Secure Shell**, and **Simple Network Management Protocol**.
6. To display the Allowed IP Addresses section, expand a service.
7. In the Allowed IP Addresses section, deselect **Allow connections from any IP address** and enter the IP addresses of networks that are allowed to connect to the host.
   Separate IP addresses with commas. You can use the following address formats:
   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64
8. Ensure that the service itself is selected.
9. Click **OK**.
10. Verify your change in the **Allowed IP addresses** column for the service.

Incoming and Outgoing Firewall Ports for ESXi Hosts

Open and close firewall ports for each service by using either the vSphere Client or the VMware Host Client.

ESXi includes a firewall that is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the host's security profile. For the list of supported ports and protocols in the ESXi firewall, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/.

The VMware Ports and Protocols Tool lists port information for services that are installed by default. If you install other VIBs on your host, additional services and firewall ports might become available. The information is primarily for services that are visible in the vSphere Client but the VMware Ports and Protocols Tool includes some other ports as well.

NFS Client Firewall Behavior

The NFS Client firewall rule set behaves differently than other ESXi firewall rule sets. ESXi configures NFS Client settings when you mount or unmount an NFS datastore. The behavior differs for different versions of NFS.

When you add, mount, or unmount an NFS datastore, the resulting behavior depends on the version of NFS.

NFS v3 Firewall Behavior

When you add or mount an NFS v3 datastore, ESXi checks the state of the NFS Client (`nfsClient`) firewall rule set.

- If the `nfsClient` rule set is disabled, ESXi enables the rule set and disables the Allow All IP Addresses policy by setting the `allowedAll` flag to `FALSE`. The IP address of the NFS server is added to the allowed list of outgoing IP addresses.
- If the `nfsClient` rule set is enabled, the state of the rule set and the allowed IP address policy are not changed. The IP address of the NFS server is added to the allowed list of outgoing IP addresses.

Note: If you manually enable the `nfsClient` rule set or manually set the Allow All IP Addresses policy, either before or after you add an NFS v3 datastore to the system, your settings are overridden when the last NFS v3 datastore is unmounted. The `nfsClient` rule set is disabled when all NFS v3 datastores are unmounted.

When you remove or unmount an NFS v3 datastore, ESXi performs one of the following actions.

- If none of the remaining NFS v3 datastores are mounted from the server of the datastore being unmounted, ESXi removes the server's IP address from the list of outgoing IP addresses.
- If no mounted NFS v3 datastores remain after the unmount operation, ESXi disables the `nfsClient` firewall rule set.

NFS v4.1 Firewall Behavior

When you mount the first NFS v4.1 datastore, ESXi enables the `nfs41client` rule set and sets its `allowedAll` flag to TRUE. This action opens port 2049 for all IP addresses. Unmounting an NFS v4.1 datastore does not affect the firewall state. That is, the first NFS v4.1 mount opens port 2049 and that port remains enabled unless you close it explicitly.

ESXi ESXCLI Firewall Commands

If your environment includes multiple ESXi hosts, automate firewall configuration by using ESXCLI commands or the vSphere Web Services SDK.

Firewall Command Reference

You can use the ESXi Shell or ESXCLI commands to configure ESXi at the command line to automate a firewall configuration. To manipulate firewalls and firewall rules, see *Getting Started with ESXCLI* for an introduction, and *ESXCLI Concepts and Examples* for examples of using ESXCLI.

In ESXi 7.0 and later, access to the `service.xml` file, used to create custom firewall rules, is restricted. See VMware Knowledge Base article 2008226 for information about creating custom firewall rules using the `/etc/rc.local.d/local.sh` file.

Table 241: Firewall Commands

Command	Description
`esxcli network firewall get`	Return the enabled or disabled status of the firewall and lists default actions.
`esxcli network firewall set --default-action`	Set to true to set the default action to pass. Set to false to set the default action to drop.
`esxcli network firewall set --enabled`	Enable or disable the ESXi firewall.
`esxcli network firewall load`	Load the firewall module and the rule set configuration files.
`esxcli network firewall refresh`	Refresh the firewall configuration by reading the rule set files if the firewall module is loaded.
`esxcli network firewall unload`	Destroy filters and unload the firewall module.
`esxcli network firewall ruleset list`	List rule sets information.
`esxcli network firewall ruleset set --allowed-all`	Set to true to allow all access to all IPs. Set to false to use a list of allowed IP addresses.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Set enabled to true to enable the specified ruleset. Set enabled to false to disable the specified ruleset.
`esxcli network firewall ruleset allowedip list`	List the allowed IP addresses of the specified rule set.
`esxcli network firewall ruleset allowedip add`	Allow access to the rule set from the specified IP address or range of IP addresses.
`esxcli network firewall ruleset allowedip remove`	Remove access to the rule set from the specified IP address or range of IP addresses.
`esxcli network firewall ruleset rule list`	List the rules of each ruleset in the firewall.

Customizing ESXi Services from the Security Profile

An ESXi host includes several services that are running by default. If your company policy allows it, you can disable services from the security profile, or enable services.

Enable or Disable a Service is an example of how to enable a service.

Note: Enabling services affects the security of your host. Do not enable a service unless strictly necessary.

Available services depend on the VIBs that are installed on the ESXi host. You cannot add services without installing a VIB. Some VMware products, for example, vSphere HA, install VIBs on hosts and make services and the corresponding firewall ports available.

In a default installation, you can modify the status of the following services from the vSphere Client.

Table 242: ESXi Services in the Security Profile

Service	Default	Description
Direct Console UI	Running	The Direct Console User Interface (DCUI) service allows you to interact with an ESXi host from the local console host using text-based menus.
ESXi Shell	Stopped	The ESXi Shell is available from the Direct Console User Interface and includes a set of fully supported commands and a set of commands for troubleshooting and remediation. You must enable access to the ESXi Shell from the direct console of each system. You can enable access to the local ESXi Shell or access to the ESXi Shell with SSH.
SSH	Stopped	The host's SSH client service that allows remote connections through Secure Shell.
Load-Based Teaming Daemon	Running	Load-Based Teaming.
attestd	Stopped	vSphere Trust Authority Attestation Service.
kmxd	Stopped	vSphere Trust Authority Key Provider Service.
Active Directory Service	Stopped	When you configure ESXi for Active Directory, this service is started.
NTP Daemon	Stopped	Network Time Protocol daemon.
PC/SC Smart Card Daemon	Stopped	When you enable the host for smart card authentication, this service starts. See Configuring Smart Card Authentication for ESXi.
CIM Server	Running	Service that can be used by Common Information Model (CIM) applications.
SNMP Server	Stopped	SNMP daemon. See *vSphere Monitoring and Performance* for information on configuring SNMP v1, v2, and v3.
Syslog Server	Stopped	Syslog daemon. You can enable syslog from the Advanced System Settings in the vSphere Client. See *vCenter Server Installation and Setup*.
VMware vCenter Agent	Running	vCenter Server agent. Allows a vCenter Server to connect to an ESXi host. Specifically, vpxa is the communication conduit to the host daemon, which in turn communicates with the ESXi kernel.
X.Org Server	Stopped	X.Org Server. This optional feature is used internally for 3D graphics for virtual machines.

Enable or Disable a Service

You can enable or disable services from the vSphere Client.

Connect to vCenter Server with the vSphere Client.

After installation, certain services are running by default, while others are stopped. Sometimes, additional setup is necessary before a service becomes available in the UI. For example, the NTP service is a way of getting accurate time information, but this service only works when required ports are opened in the firewall.

1. Browse to a host in the inventory.
2. Click **Configure**, then click **Services** under System.
3. Select the service you want to change.
   a) Select **Restart**, **Start**, or **Stop** for a one-time change to the host's status.
   b) To change the status of the host across reboots, click **Edit Startup Policy** and select a policy.

   - **Start and stop with host**: The service starts shortly after the host starts, and closes shortly before the host shuts down. Much like **Start and stop with port usage**, this option means that the service regularly attempts to complete its tasks, such as contacting the specified NTP server. If the port was closed but is later opened, the client begins completing its tasks shortly thereafter.
   - **Start and stop manually**: The host preserves the user-determined service settings, regardless of whether ports are open or not. When a user starts the NTP service, that service is kept running if the host is powered on. If the service is started and the host is powered off, the service is stopped as part of the shutdown process. When the host is powered on, the service is started again, preserving the user-determined state.
   - **Start and stop with port usage**: The default setting for these services. If any port is open, the client attempts to contact the network resources for the service. If some ports are open, but the port for a particular service is closed, the attempt fails. If and when the applicable outgoing port is opened, the service begins completing its startup.

   Note: These settings apply only to service settings that are configured through the UI or to applications that are created with the vSphere Web Services SDK. Configurations made through other means, such as from the ESXi Shell or with configuration files, are not affected by these settings.
4. Click **OK**.

Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode. In lockdown mode, operations must be performed through vCenter Server by default.

You can select normal lockdown mode or strict lockdown mode, which offer different degrees of lockdown. You can also use the Exception User list. Exception users do not lose their privileges when the host enters lockdown mode. Use the Exception User list to add the accounts of third-party solutions and external applications that need to access the host directly when the host is in lockdown mode. See Specify Lockdown Mode Exception Users.

Lockdown Mode Behavior

In lockdown mode, some services are disabled, and some services are accessible only to certain users.

Lockdown Mode Services for Different Users

When the host is running, available services depend on whether lockdown mode is enabled, and on the type of lockdown mode.

- In strict and normal lockdown mode, privileged users can access the host through vCenter Server, from the vSphere Client, or by using the vSphere Web Services SDK.

- Direct Console Interface behavior differs for strict lockdown mode and normal lockdown mode.
  - In strict lockdown mode, the Direct Console User Interface (DCUI) service is disabled.
  - In normal lockdown mode, accounts on the Exception User list can access the DCUI if they have administrator privileges. In addition, all users who are specified in the `DCUI.Access` advanced system setting can access the DCUI.
- If the ESXi Shell or SSH is enabled and the host is placed in lockdown mode, accounts on the Exception Users list who have administrator privileges can use these services. For all other users, ESXi Shell or SSH access is disabled. ESXi or SSH sessions for users who do not have administrator privileges are closed.

All access is logged for both strict and normal lockdown mode.

Table 243: Lockdown Mode Behavior

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
Direct Console UI (DCUI)	Users with administrator privileges on the host, and users in the `DCUI.Access` advanced option	Users defined in the `DCUI.Access` advanced option Exception users with administrator privileges on the host	DCUI service is stopped.
ESXi Shell (if enabled) and SSH (if enabled)	Users with administrator privileges on the host	Users defined in the `DCUI.Access` advanced option Exception users with administrator privileges on the host	Users defined in the `DCUI.Access` advanced option Exception users with administrator privileges on the host

Users Logged In to the ESXi Shell When Lockdown Mode Is Enabled

Users might log in to the ESXi Shell or access the host through SSH before lockdown mode is enabled. In that case, users who are on the list of Exception Users and who have administrator privileges on the host remain logged in. The session is closed for all other users. Termination applies to both normal and strict lockdown mode.

Enable Lockdown Mode

Enable lockdown mode to require that all configuration changes go through vCenter Server. vSphere 6.0 and later supports normal lockdown mode and strict lockdown mode.

If you want to disallow all direct access to a host completely, you can select strict lockdown mode. Strict lockdown mode makes it impossible to access a host if the vCenter Server is unavailable and SSH and the ESXi Shell are disabled. See Lockdown Mode Behavior.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Security Profile**.
4. In the Lockdown Mode panel, click **Edit**.
5. Click **Lockdown Mode** and select one of the lockdown mode options.

Option	Description
Normal	The host can be accessed through vCenter Server. Only users who are on the Exception Users list and have administrator privileges can log in to the Direct Console User Interface. If SSH or the ESXi Shell is enabled, access might be possible.
Strict	The host can only be accessed through vCenter Server. If SSH or the ESXi Shell is enabled, running sessions for accounts in the `DCUI.Access` advanced option and for Exception User accounts that have administrator privileges remain enabled. All other sessions are closed.

6. Click **OK**.

Disable Lockdown Mode

Disable lockdown mode to allow configuration changes from direct connections to the ESXi host. Leaving lockdown mode enabled results in a more secure environment.

You can disable lockdown mode as follows:

From the Graphical User Interface	Users can disable both normal lockdown mode and strict lockdown mode from the vSphere Client.
From the Direct Console User Interface	Users who can access the Direct Console User Interface on the ESXi host can disable normal lockdown mode. In strict lockdown mode, the Direct Console Interface service is stopped.

1. Browse to a host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Security Profile**.
4. In the Lockdown Mode panel, click **Edit**.
5. Click **Lockdown Mode** and select **Disabled** to disable lockdown mode.
6. Click **OK**.

The system exits lockdown mode, vCenter Server displays an alarm, and an entry is added to the audit log.

Enable or Disable Normal Lockdown Mode from the Direct Console User Interface

You can enable and disable normal lockdown mode from the Direct Console User Interface (DCUI). You can enable and disable strict lockdown mode only from the vSphere Client.

When the host is in normal lockdown mode, the following accounts can access the Direct Console User Interface:

- Accounts in the Exception Users list who have administrator privileges on the host. The Exception Users list is meant for service accounts such as a backup agent.
- Users defined in the `DCUI.Access` advanced option for the host. This option can be used to enable access in a catastrophic failure.

User permissions are preserved when you enable lockdown mode. User permissions are restored when you disable lockdown mode from the Direct Console Interface.

Note: If you upgrade a host that is in lockdown mode to ESXi version 6.0 without exiting lockdown mode, and if you exit lockdown mode after the upgrade, all permissions defined before the host entered lockdown mode are lost. The system assigns the administrator role to all users who are found in the `DCUI.Access` advanced option to guarantee that the host remains accessible.

To retain permissions, disable lockdown mode for the host from the vSphere Client before the upgrade.

1. At the Direct Console User Interface of the host, press F2 and log in.
2. Scroll to the **Configure Lockdown Mode** setting and press Enter to toggle the current setting.
3. Press Esc until you return to the main menu of the Direct Console User Interface.

Specifying Accounts with Access Privileges in Lockdown Mode

You can specify service accounts that can access the ESXi host directly by adding them to the Exception Users list. You can specify a single user who can access the ESXi host in a catastrophic vCenter Server failure.

The vSphere version determines what different accounts can do by default when lockdown mode is enabled, and how you can change the default behavior.

- In vSphere 5.0 and earlier, only the root user can log in to the Direct Console User Interface on an ESXi host that is in lockdown mode.
- In vSphere 5.1 and later, you can add a user to the `DCUI.Access` advanced system setting for each host. The option is meant for a catastrophic failure of vCenter Server. Companies usually lock the password for the user with this access into a safe. A user in the `DCUI.Access` list does not need to have full administrative privileges on the host.
- In vSphere 6.0 and later, the `DCUI.Access` advanced system setting is still supported. In addition, vSphere 6.0 and later supports an Exception User list, which is for service accounts that have to log in to the host directly. Accounts with administrator privileges that are on the Exception Users list can log in to the ESXi Shell. In addition, those users can log in to a host's DCUI in normal lockdown mode and can exit lockdown mode.

  You specify Exception Users from the vSphere Client.

  Note: Exception users are host local users or Active Directory users with privileges defined locally for the ESXi host. Users that are members of an Active Directory group lose their permissions when the host is in lockdown mode.

Add Users to the DCUI.Access Advanced Option

If there is a catastrophic failure, the `DCUI.Access` advanced option allows you to exit lockdown mode when you cannot access the host from vCenter Server. You add users to the list by editing the Advanced Settings for the host from the vSphere Client.

Note: Users in the DCUI.Access list can change lockdown mode settings regardless of their privileges. The ability to change lockdown modes can impact the security of your host. For service accounts that need direct access to the host,

consider adding users to the Exception Users list instead. Exception users can only perform tasks for which they have privileges. See Specify Lockdown Mode Exception Users.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, click **Advanced System Settings**, and click **Edit**.
4. Filter for DCUI.
5. In the **DCUI.Access** text box, enter the local ESXi user names, separated by commas.

   Note: You cannot enter Active Directory users. Only local ESXi users are supported.

   By default, the root user is included. Consider removing the root user from the DCUI.Access list, and specifying a named account for better auditability.
6. Click **OK**.

Specify Lockdown Mode Exception Users
You can add users to the Exception Users list from the vSphere Client. These users do not lose their permissions when the host enters lockdown mode. It makes sense to add service accounts such as a backup agent to the Exception Users list.

Exception users do not lose their privileges when the host enters lockdown mode. Usually these accounts represent third-party solutions and external applications that need to continue to function in lockdown mode.

Note: The Exception Users list is meant for service accounts that perform very specific tasks, and not for administrators. Adding administrator users to the Exception Users list defeats the purpose of lockdown mode.

Exception users are host local users or Active Directory users with privileges defined locally for the ESXi host. They are not members of an Active Directory group and are not vCenter Server users. These users are allowed to perform operations on the host based on their privileges. That means, for example, that a read-only user cannot disable lockdown mode on a host.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Security Profile**.
4. In the Lockdown Mode panel, click **Edit**.
5. Click **Exception Users** and click the **Add User** icon to add exception users.

Using VIBs to Perform Secure Updates

Upgrading ESXi with ESXCLI requires an understanding of VIBs, image profiles, and software depots.

ESXi consists of an image profile, which describes a set of vSphere Installation Bundles (VIBs) that contain the actual software. A VIB is a signed ramdisk representing a component of the system, roughly analogous to an RPM or DEB on a Linux system. An image profile is a collection of VIBs. A software depot is a collection of VIBs and image profiles. ESXi patches and depots contain updated image profiles composed from a common set of VIBs.

You can install ESXi updates on a standalone host using the `esxcli software` commands. For more information, see the *VMware ESXi Upgrade* documentation.

Note: Normally, in a vSphere 7.0 and later environment, you use VMware vSphere® vSphere Lifecycle Manager for lifecycle management of ESXi hosts.

To list all installed VIBs and their current version, or the current image profile, you can use the following ESXCLI commands.

- `esxcli software vib list`
- `esxcli software profile get`

In general, the high-level steps to upgrade ESXi securely are:

- Putting the ESXi host in maintenance mode
- Running an `esxcli software profile update` command, which points to a URL or a ZIP file transferred to the host through SSH
- Restarting the ESXi host

Because VMware cryptographically signs VIBS, secure transfer of VIBs or the entire depot is not necessary, and the update process verifies these signatures.

Manage the Acceptance Levels of Hosts and VIBs

The acceptance level of a VIB depends on the amount of certification of that VIB. The acceptance level of the host depends on the level of the lowest VIB. If you want to allow lower-level VIBs, you can change the acceptance level of the host. You can remove CommunitySupported VIBs to be able to change the host acceptance level.

VIBs are software packages that include a signature from VMware or a VMware partner. To protect the integrity of the ESXi host, do not allow users to install unsigned (community-supported) VIBs. An unsigned VIB contains code that is not certified by, accepted by, or supported by VMware or its partners. Community-supported VIBs do not have a digital signature.

The host's acceptance level must be the same or less restrictive than the acceptance level of any VIB you want to add to the host. For example, if the host acceptance level is VMwareAccepted, you cannot install VIBs at the PartnerSupported level. You can use ESXCLI commands to set an acceptance level for a host. To protect the security and integrity of your ESXi hosts, do not allow unsigned (CommunitySupported) VIBs to be installed on hosts in production systems.

The acceptance level for an ESXi host is displayed in the **Security Profile** in the vSphere Client.

The following acceptance levels are supported.

VMwareCertified	The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only I/O Vendor Program (IOVP) program drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.
VMwareAccepted	VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plug-ins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
PartnerSupported	VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
CommunitySupported	The CommunitySupported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs. VIBs at this level have not gone through any VMware-approved

testing program and are not supported by VMware Technical Support or by a VMware partner.

1. Connect to each ESXi host and verify that the acceptance level is set to VMwareCertified, VMwareAccepted, or PartnerSupported by running the following command.

   ```
   esxcli software acceptance get
   ```

2. If the host acceptance level is CommunitySupported, determine whether any of the VIBs are at the CommunitySupported level by running the following commands.

   ```
   esxcli software vib list
   esxcli software vib get -n vibname
   ```

3. Remove any CommunitySupported VIBs by running the following command.

   ```
   esxcli software vib remove --vibname vib
   ```

4. Change the acceptance level of the host by using one of the following methods.

Option	Description
CLI command	`esxcli software acceptance set --level level` The `level` parameter is required and specifies the acceptance level to set. Should be one of `VMwareCertified`, `VMwareAccepted`, `PartnerSupported`, or `CommunitySupported`. See *ESXCLI Reference* for more information.
vSphere Client	1. Select a host in the inventory. 2. Click **Configure**. 3. Under System, select **Security Profile**. 4. Click **Edit** for Host Image Profile Acceptance Level and choose the acceptance level.

The new acceptance level is in effect.

Note:

ESXi conducts integrity checks of VIBs governed by the Acceptance Level. You can use the `VMkernel.Boot.execInstalledOnly` setting to instruct ESXi to only execute binaries that originate from a valid VIB installed on the host. Combined with Secure Boot, this setting ensures that every single process ever run on an ESXi host is signed, allowed, and expected. By default, the `VMkernel.Boot.execInstalledOnly` setting is disabled for partner compatibility in vSphere 7. Enabling this setting when possible improves security. For more information on configuring advanced options for ESXi, see the VMware knowledge base article at https://kb.vmware.com/kb/1038578.

Assigning Privileges for ESXi Hosts

Usually, you give privileges to users by assigning permissions to ESXi host objects that are managed by a vCenter Server system. If you are using a standalone ESXi host, you can assign privileges directly.

Assigning Permissions to ESXi Hosts That Are Managed by vCenter Server

If your ESXi host is managed by a vCenter Server, perform management tasks through the vSphere Client.

You can select the ESXi host object in the vCenter Server object hierarchy and assign the administrator role to a limited number of users. Those users can then perform direct management on the ESXi host. See Using Roles to Assign Privileges.

Best practice is to create at least one named user account, assign it full administrative privileges on the host, and use this account instead of the root account. Set a highly complex password for the root account and limit the use of the root account. Do not remove the root account.

Assigning Permissions to Standalone ESXi Hosts

You can add local users and define custom roles from the Management tab of the VMware Host Client. See the *vSphere Single Host Management - VMware Host Client* documentation.

For all versions of ESXi, you can see the list of predefined users in the `/etc/passwd` file.

The following roles are predefined.

Read Only	Allows a user to view objects associated with the ESXi host but not to make any changes to objects.
Administrator	Administrator role.
No Access	No access. This role is the default role. You can override the default role.

You can manage local users and groups and add local custom roles to an ESXi host using a VMware Host Client connected directly to the ESXi host. See the *vSphere Single Host Management - VMware Host Client* documentation.

Starting with vSphere 6.0, you can use ESXCLI account management commands for managing ESXi local user accounts. You can use ESXCLI permission management commands for setting or removing permissions on both Active Directory accounts (users and groups) and on ESXi local accounts (users only).

Note: If you define a user for the ESXi host by connecting to the host directly, and a user with the same name also exists in vCenter Server, those users are different. If you assign a role to the ESXi user, the vCenter Server user is not assigned the same role.

Predefined Privileges

If your environment does not include a vCenter Server system, the following users are predefined.

root User	By default each ESXi host has a single root user account with the Administrator role. That root user account can be used for local administration and to connect the host to vCenter Server. Assigning root user privileges can make it easier to break into an ESXi host because the name is already known. Having a common root account also makes it harder to match actions to users. For better auditing, create individual accounts with Administrator privileges. Set a highly complex password for the root account and limit the use of the root account, for example, for use when adding a host to vCenter Server. Do not remove the root account. For more information about assigning permissions to a user for an ESXi host, see *vSphere Single Host Management - VMware Host Client* documentation. Best practice is to ensure that any account with the Administrator role on an ESXi host is assigned to a specific user with a named account. Use ESXi Active Directory capabilities, which allow you to manage Active Directory credentials. **Important:** You can remove the access privileges for the root user. However, you must first create another permission at the root level that has a different user assigned to the Administrator role.
vpxuser User	vCenter Server uses vpxuser privileges when managing activities for the host. The vCenter Server administrator can perform most of the same tasks on the host as the root user and also schedule tasks, work with templates, and so forth. However, the vCenter Server administrator cannot directly create, delete, or edit local users and

	groups for hosts. Only a user with Administrator privileges can perform these tasks directly on a host. **Note:** You cannot manage vpxuser using Active Directory. **CAUTION:** Do not change vpxuser in any way. Do not change its password. Do not change its permissions. If you do so, you might experience problems when working with hosts through vCenter Server.
dcui User	The dcui user runs on hosts and acts with Administrator rights. This user's primary purpose is to configure hosts for lockdown mode from the Direct Console User Interface (DCUI). This user acts as an agent for the direct console and cannot be modified or used by interactive users.

Using Active Directory to Manage ESXi Users

You can configure ESXi to use a directory service such as Active Directory to manage users.

Creating local user accounts on each host presents challenges with having to synchronize account names and passwords across multiple hosts. Join ESXi hosts to an Active Directory domain to eliminate the need to create and maintain local user accounts. Using Active Directory for user authentication simplifies the ESXi host configuration and reduces the risk for configuration issues that could lead to unauthorized access.

When you use Active Directory, users supply their Active Directory credentials and the domain name of the Active Directory server when adding a host to a domain.

Configure a Host to Use Active Directory

You can configure a host to use a directory service such as Active Directory to manage users and groups.

- Verify that you have an Active Directory domain. See your directory server documentation.
- Verify that the host name of ESXi is fully qualified with the domain name of the Active Directory forest.
  `fully qualified domain name` = *`host_name.domain_name`*

When you add an ESXi host to Active Directory, the DOMAIN group **ESX Admins** is assigned full administrative access to the host if it exists. If you do not want to make full administrative access available, see VMware Knowledge Base article 1025569 for a workaround.

If a host is provisioned with Auto Deploy, Active Directory credentials cannot be stored on the hosts. You can use the vSphere Authentication Proxy to join the host to an Active Directory domain. Because a trust chain exists between the vSphere Authentication Proxy and the host, the Authentication Proxy can join the host to the Active Directory domain. See Using vSphere Authentication Proxy.

Note: When you define user account settings in Active Directory, you can limit the computers that a user can log in to by the computer name. By default, no equivalent restrictions are set on a user account. If you set this limitation, LDAP Bind requests for the user account fail with the message `LDAP binding not successful`, even if the request is from a listed computer. You can avoid this problem by adding the netBIOS name for the Active Directory server to the list of computers that the user account can log in to.

1. Synchronize the time between ESXi and the directory service system.

   See Synchronize ESXi Clocks with a Network Time Server or the VMware Knowledge Base for information about how to synchronize ESXi time with a Microsoft Domain Controller.

2. Ensure that the DNS servers that you configured for the host can resolve the host names for the Active Directory controllers.
   a) Browse to the host in the vSphere Client inventory.
   b) Click **Configure**.
   c) Under Networking, click **TCP/IP configuration**.
   d) Under TCP/IP Stack: Default, click **DNS** and verify that the host name and DNS server information for the host are correct.

Join the host to a directory service domain. See Add a Host to a Directory Service Domain. For hosts that are provisioned with Auto Deploy, set up the vSphere Authentication Proxy. See Using vSphere Authentication Proxy. You can configure permissions so that users and groups from the joined Active Directory domain can access the vCenter Server components. For information about managing permissions, see Add a Permission to an Inventory Object .

Add a Host to a Directory Service Domain

To have your host use a directory service, you must join the host to the directory service domain.

You can enter the domain name in one of two ways:

- `name.tld` (for example, `domain.com`): The account is created under the default container.
- `name.tld/container/path` (for example, `domain.com/OU1/OU2`): The account is created under a particular organizational unit (OU).

To use the vSphere Authentication Proxy service, see Using vSphere Authentication Proxy.

1. Browse to a host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Authentication Services**.
4. Click **Join Domain**.
5. Enter a domain.

   Use the form `name.tld` or `name.tld/container/path`.
6. Enter the user name and password of a directory service user who has permissions to join the host to the domain, and click **OK**.
7. Optional: If you intend to use an authentication proxy, enter the proxy server IP address.
8. Click **OK** to close the Directory Services Configuration dialog box.

You can configure permissions so that users and groups from the joined Active Directory domain can access the vCenter Server components. For information about managing permissions, see Add a Permission to an Inventory Object .

View Directory Service Settings

You can view the type of directory server, if any, that the host uses to authenticate users and the directory server settings.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Authentication Services**.

   The Authentication Services page displays the directory service and domain settings.

You can configure permissions so that users and groups from the joined Active Directory domain can access the vCenter Server components. For information about managing permissions, see Add a Permission to an Inventory Object .

Using vSphere Authentication Proxy

You can add ESXi hosts to an Active Directory domain by using vSphere Authentication Proxy instead of adding the hosts explicitly to the Active Directory domain.

You only have to set up the host so it knows about the domain name of the Active Directory server and about the IP address of vSphere Authentication Proxy. When vSphere Authentication Proxy is enabled, it automatically adds hosts that are being provisioned with Auto Deploy to the Active Directory domain. You can also use vSphere Authentication Proxy with hosts that are not provisioned by using Auto Deploy.

Auto Deploy	If you are provisioning hosts with Auto Deploy, you can set up a reference host that points to Authentication Proxy. You then set up a rule that applies the reference host's profile to any ESXi host that is provisioned with Auto Deploy. vSphere Authentication Proxy stores the IP addresses of all hosts that Auto Deploy provisions using PXE in its access control list. When the host boots, it contacts vSphere Authentication Proxy, and vSphere Authentication Proxy joins those hosts, which are already in its access control list, to the Active Directory domain. Even if you use vSphere Authentication Proxy in an environment that uses certificates that are provisioned by VMCA or third-party certificates, the process works seamlessly if you follow the instructions for using custom certificates with Auto Deploy.
Other ESXi Hosts	You can set up other hosts to use vSphere Authentication Proxy if you want to make it possible for the host to join the domain without using Active Directory credentials. That means you do not need to transmit Active Directory credentials to the host, and you do not save Active Directory credentials in the host profile. In that case, you add the host's IP address to the vSphere Authentication Proxy access control list, and vSphere Authentication Proxy authorizes the host based on its IP address by default. You can enable client authentication to have vSphere Authentication Proxy check the host's certificate.

Note: You cannot use vSphere Authentication Proxy in an environment that supports only IPv6.

Enable vSphere Authentication Proxy

The vSphere Authentication Proxy service is available on each vCenter Server system. By default, the service is not running. If you want to use vSphere Authentication Proxy in your environment, you can start the service from the vCenter Server Management Interface or from the command line.

Verify that you are using vCenter Server 6.5 or later. In earlier versions of vSphere, vSphere Authentication Proxy is installed separately. See the documentation for the earlier version of the product for instructions.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server instance can be on a host machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment. However, when you specify the address of vSphere Authentication Proxy, you must specify an IPv4 address.

1. Start the VMware vSphere Authentication Proxy service.

Option	Description
vCenter Server Management Interface	1. In a Web browser, go to the vCenter Server Management Interface, https://*vcenter-IP-address-or-FQDN*:5480. 2. Log in as root. The default root password is the password that you set while deploying the vCenter Server. 3. Click **Services**, and click the **VMware vSphere Authentication Proxy** service.

Option	Description
	4. Click **Start**. 5. After the service has started, click **Set Startup Type** and click **Automatic** to make the startup automatic.
CLI	`service-control --start vmcam`

2. Confirm that the service started successfully.

You can now set the vSphere Authentication Proxy domain. After that, vSphere Authentication Proxy handles all hosts that are provisioned with Auto Deploy, and you can explicitly add hosts to vSphere Authentication Proxy.

Add a Domain to vSphere Authentication Proxy with the vSphere Client

You can add a domain to vSphere Authentication Proxy from the vSphere Client or by using the `camconfig` command.

You can add a domain to vSphere Authentication Proxy only after you enable the proxy. After you add the domain, vSphere Authentication Proxy adds all hosts that you provision with Auto Deploy to that domain. For other hosts, you can also use vSphere Authentication Proxy if you do not want to give those hosts domain privileges.

1. Connect to a system with the .
2. Select the , and click **Configure**.
3. Click **Authentication Proxy** and click **Edit**.
4. Enter the name of the domain that vSphere Authentication Proxy will add hosts to, and the name and password of a user who has Active Directory privileges to add hosts to the domain.
5. Click **Save**.

Add a Domain to vSphere Authentication Proxy with the camconfig Command

You can add a domain to vSphere Authentication using the `camconfig` command.

You can add a domain to vSphere Authentication Proxy only after you enable the proxy. After you add the domain, vSphere Authentication Proxy adds all hosts that you provision with Auto Deploy to that domain. For other hosts, you can also use vSphere Authentication Proxy if you do not want to give those hosts domain privileges.

1. Log in to the system as a user with administrator privileges.
2. Run the command to enable access to the Bash shell.

   ```
   shell
   ```

3. Go to the `/usr/lib/vmware-vmcam/bin/` directory where the **camconfig** script is located.
4. To add the domain and user Active Directory credentials to the Authentication Proxy configuration, run the following command.

   ```
   camconfig add-domain -d domain -u user
   ```

   You are prompted for a password.

   vSphere Authentication Proxy caches that user name and password. You can remove and recreate the user as needed. The domain must be reachable through DNS, but does not have to be a vCenter Single Sign-On identity source.

   vSphere Authentication Proxy uses the user name specified by *`user`* to create the accounts for ESXi hosts in Active Directory. The user must have privileges to create accounts in the Active Directory domain to which you are adding the hosts. At the time of writing of this information, the Microsoft Knowledge Base article 932455 had background information for account creation privileges.

5. If you later want to remove the domain and user information from vSphere Authentication Proxy, run the following command.

   ```
   camconfig remove-domain -d domain
   ```

Use vSphere Authentication Proxy to Add a Host to a Domain

The Auto Deploy server adds all hosts that it provisions to vSphere Authentication Proxy, and vSphere Authentication Proxy adds those hosts to the domain. If you want to add other hosts to a domain using vSphere Authentication Proxy, you can add those hosts to vSphere Authentication Proxy explicitly. Afterwards, the vSphere Authentication Proxy server adds those hosts to the domain. As a result, user-supplied credentials no longer have to be transmitted to the vCenter Server system.

- If the ESXi host is using a VMCA-signed certificate, verify that the host has been added to vCenter Server. Otherwise, the Authentication Proxy service cannot trust the ESXi host.
- If the ESXi host is using a root CA-signed certificate, verify that the appropriate root CA-signed certificate has been added to the vCenter Server system. See Certificate Management for ESXi Hosts.

You can enter the domain name in one of two ways:

- `name.tld` (for example, `domain.com`): The account is created under the default container.
- `name.tld/container/path` (for example, `domain.com/OU1/OU2`): The account is created under a particular organizational unit (OU).

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under **System**, select **Authentication Services**.
4. Click **Join Domain**.
5. Enter a domain.

   Use the form `name.tld`, for example `mydomain.com`, or `name.tld/container/path`, for example, `mydomain.com/organizational_unit1/organizational_unit2`.
6. Select **Using Proxy Server**.
7. Enter the IP address of the Authentication Proxy server, which is always the same as the IP address of the vCenter Server system.
8. Click **OK**.

Enable Client Authentication for vSphere Authentication Proxy

By default, vSphere Authentication Proxy adds any host if it has the IP address of that host in its access control list. For additional security, you can enable client authentication. If client authentication is enabled, vSphere Authentication Proxy also checks the certificate of the host.

- Verify that the system trusts the host. By default, when you add a host to , the host is assigned a certificate that is signed by a trusted root CA. vSphere Authentication Proxy trusts trusted root CA.
- If you plan on replacing ESXi certificates in your environment, perform the replacement before you enable vSphere Authentication Proxy. The certificates on the ESXi host must match that of the host's registration.

1. Log in to the system as a user with administrator privileges.
2. Run the command to enable access to the Bash shell.

   ```
   shell
   ```

3. Go to the `/usr/lib/vmware-vmcam/bin/` directory where the **camconfig** script is located.
4. Run the following command to enable client authentication.

   ```
   camconfig ssl-cliAuth -e
   ```

   Going forward, vSphere Authentication Proxy checks the certificate of each host that is added.
5. If you later want to disable client authentication again, run the following command.

   ```
   camconfig ssl-cliAuth -n
   ```

Import the vSphere Authentication Proxy Certificate to ESXi Host

By default, ESXi hosts require explicit verification of the vSphere Authentication Proxy certificate. If you are using vSphere Auto Deploy, the Auto Deploy service takes care of adding the certificate to hosts that it provisions. For other hosts, you must add the certificate explicitly.

- Upload the vSphere Authentication Proxy certificate to a datastore accessible to the ESXi host. Using an SFTP application such WinSCP, you can download the certificate from the vCenter Server host at the following location.
  `/var/lib/vmware/vmcam/ssl/rui.crt`
- Verify that the UserVars.ActiveDirectoryVerifyCAMCertificateESXi advanced setting is set to 1 (the default).

1. Select the ESXi host and click **Configure**.
2. Under **System**, select **Authentication Services**.
3. Click **Import Certificate**.
4. Enter the certificate file path following the format `[`*`datastore`*`]`*`/path/certname`*`.crt`, and click **OK**.

Generate a New Certificate for vSphere Authentication Proxy

You can generate a new certificate that is provisioned by VMCA, or a new certificate that includes VMCA as a subordinate certificate.

You must have root or Administrator privileges on the system on which vSphere Authentication Proxy is running.

See Set Up vSphere Authentication Proxy to Use Custom Certificates if you want to use a custom certificate that is signed by a third-party or enterprise CA.

1. Make a copy of `certool.cfg`.

   ```
   cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
   ```

2. Edit the copy with some information about your organization, as in the following example.

   ```
   Country = IE
   Name = vmcam
   Organization = VMware
   OrgUnit = vTSU
   State = Cork
   Locality = Cork
   Hostname = test-cam-1.test1.vmware.com
   ```

3. Generate the new private key in `/var/lib/vmware/vmcam/ssl/`.

   ```
   /usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --pubkey=/tmp/vm-cam.pub --server=localhost
   ```

   For *`localhost`*, supply the FQDN of the vCenter Server.

4. Generate the new certificate in `/var/lib/vmware/vmcam/ssl/` using the key and `vmcam.cfg` file that you created in Step 1 and Step 2.

   ```
   /usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --privkey=/var/lib/vmware/vmcam/ssl/rui.key
    --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/vmcam/ssl/vmcam.cfg
   ```

   For *localhost*, supply the FQDN of the vCenter Server.

Set Up vSphere Authentication Proxy to Use Custom Certificates

Using custom certificates with vSphere Authentication Proxy consists of several steps. First you generate a CSR and send it to your CA for signing. Then you place the signed certificate and key file in a location that vSphere Authentication Proxy can access.

By default, vSphere Authentication Proxy generates a CSR during first boot and asks VMCA to sign that CSR. vSphere Authentication Proxy registers with using that certificate. You can use custom certificates in your environment, if you add those certificates to .

1. Generate a CSR for vSphere Authentication Proxy.
   a) Create a configuration file, `/var/lib/vmware/vmcam/ssl/vmcam.cfg`, as in the following example.

      ```
      [ req ]
      distinguished_name = req_distinguished_name
      encrypt_key = no
      prompt = no
      string_mask = nombstr
      req_extensions = v3_req
      [ v3_req ]
      basicConstraints = CA:false
      keyUsage = nonRepudiation, digitalSignature, keyEncipherment
      subjectAltName = DNS:vcenter1.example.com
      [ req_distinguished_name ]
      countryName = US
      stateOrProvinceName = NY
      localityName = New York
      0.organizationName = Example Inc.
      organizationalUnitName = IT Org
      commonName = vcenter1.example.com
      ```

      Note the following:

      - subjectAltName: Use the format `DNS:`*`FQDN_of_vCenter_Appliance_to_use_the_CA-signed certificate`*.
      - commonName: Use the same FQDN of the vCenter Appliance used in subjectAltName.

   b) Run `openssl` to generate a CSR file and a key file, passing in the configuration file.

      ```
      openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/vmcam/ssl/rui.key -con-
      fig /var/lib/vmware/vmcam/ssl/vmcam.cfg
      ```

2. Back up the `rui.crt` certificate and `rui.key` files, which are stored in the following location.
   `/var/lib/vmware/vmcam/ssl/rui.crt`
3. Unregister vSphere Authentication Proxy.
   a) Go to the `/usr/lib/vmware-vmcam/bin` directory where the `camregister` script is located.
   b) Run the following command.

      ```
      camregister --unregister -a VC_address -u user
      ```

      user must be a vCenter Single Sign-On user that has administrator permissions on .

4. Stop the vSphere Authentication Proxy service.

Tool	Steps
Configuration Management Interface	1. In a Web browser, go to the Configuration Management Interface, https://*vcenter-IP-address-or-FQDN*:5480. 2. Log in as root. The default root password is the password that you set while deploying the . 3. Click **Services**, and click the **VMware vSphere Authentication Proxy service**. 4. Click **Stop**.
CLI	`service-control --stop vmcam`

5. Replace the existing `rui.crt` certificate and `rui.key` files with the files that you received from your CA.
6. Restart the vSphere Authentication Proxy service.
7. Reregister vSphere Authentication Proxy explicitly with by using the new certificate and key.

   `camregister --register -a VC_address -u user -c` *`full_path_to_rui.crt`* `-k` *`full_path_to_rui.key`*

Configuring Smart Card Authentication for ESXi

You can use smart card authentication to log in to the ESXi Direct Console User Interface (DCUI) by using a Personal Identity Verification (PIV), Common Access Card (CAC) or SC650 smart card instead specifying a user name and password.

A smart card is a small plastic card with an embedded integrated circuit chip. Many government agencies and large enterprises use smart card based two-factor authentication to increase the security of their systems and comply with security regulations.

When smart card authentication is enabled on an ESXi host, the DCUI prompts for a smart card and PIN combination instead of the default prompt for a user name and password.

1. When you insert the smart card into the smart card reader, the ESXi host reads the credentials on it.
2. The ESXi DCUI displays your login ID, and prompts for your PIN.
3. After you enter your PIN, the ESXi host matches it with the PIN stored on the smart card and verifies the certificate on the smart card with Active Directory.
4. After successful verification of the smart card certificate, ESXi logs you in to the DCUI.

You can switch to user name and password authentication from the DCUI by pressing F3.

The chip on the smart card locks after a few consecutive incorrect PIN entries, usually three. If a smart card is locked, only selected personnel can unlock it.

Enable Smart Card Authentication

Enable smart card authentication to prompt for smart card and PIN combination to log in to the ESXi DCUI.

- Set up the infrastructure to handle smart card authentication, such as accounts in the Active Directory domain, smart card readers, and smart cards.

- Configure ESXi to join an Active Directory domain that supports smart card authentication. For more information, see Using Active Directory to Manage ESXi Users .
- Use the vSphere Client to add root certificates. See Certificate Management for ESXi Hosts.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Authentication Services**.
   You see the current smart card authentication status and a list with imported certificates.
4. In the Smart Card Authentication panel, click **Edit**.
5. In the Edit Smart Card Authentication dialog box, select the Certificates page.
6. Add trusted Certificate Authority (CA) certificates, for example, root and intermediary CA certificates.
   Certificates must be in PEM format.
7. Open the Smart Card Authentication page, select the **Enable Smart Card Authentication** check box, and click **OK**.

Disable Smart Card Authentication

Disable smart card authentication to return to the default user name and password authentication for ESXi DCUI login.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Authentication Services**.
   You see the current smart card authentication status and a list with imported certificates.
4. In the Smart Card Authentication panel, click **Edit**.
5. On the Smart Card Authentication page, deselect the **Enable Smart Card Authentication** check box, and click **OK**.

Authenticating With User Name and Password in Case of Connectivity Problems

If the Active Directory (AD) domain server is not reachable, you can log in to the ESXi DCUI by using user name and password authentication to perform emergency actions on the host.

In exceptional circumstances, the AD domain server is not reachable to authenticate the user credentials on the smart card because of connectivity problems, network outage, or disasters. In that case, you can log in to the ESXi DCUI by using the credentials of a local ESXi Administrator user. After logging in, you can perform diagnostics or other emergency actions. The fallback to user name and password login is logged. When the connectivity to AD is restored, smart card authentication is enabled again.

Note: Loss of network connectivity to vCenter Server does not affect smart card authentication if the Active Directory (AD) domain server is available.

Using Smart Card Authentication in Lockdown Mode

When enabled, lockdown mode on the ESXi host increases the security of the host and limits access to the DCUI. Lockdown mode might disable the smart card authentication feature.

In normal lockdown mode, only users on the Exception Users list with administrator privileges can access the DCUI. Exception users are host local users or Active Directory users with permissions defined locally for the ESXi host. If you want to use smart card authentication in normal lockdown mode, you must add users to the Exception Users list from the vSphere Client. These users do not lose their permissions when the host enters normal lockdown mode and can log in to the DCUI. For more information, see Specify Lockdown Mode Exception Users.

In strict lockdown mode, the DCUI service is stopped. As a result, you cannot access the host by using smart card authentication.

Using the ESXi Shell

The ESXi Shell is disabled by default on ESXi hosts. You can enable local and remote access to the shell if necessary.

To reduce the risk of unauthorized access, enable the ESXi Shell for troubleshooting only.

The ESXi Shell is independent of lockdown mode. Even if the host is running in lockdown mode, you can still log in to the ESXi Shell if it is enabled.

ESXi Shell	Enable this service to access the ESXi Shell locally.
SSH	Enable this service to access the ESXi Shell remotely by using SSH.

The root user and users with the Administrator role can access the ESXi Shell. Users who are in the Active Directory group ESX Admins are automatically assigned the Administrator role. By default, only the root user can run system commands (such as `vmware -v`) by using the ESXi Shell.

Note: Do not enable the ESXi Shell unless you actually need access.

Enable Access to the ESXi Shell

ESXi Shell and SSH interfaces are disabled by default. Keep these interfaces disabled unless you are performing troubleshooting or support activities. For day-to-day activities, use the vSphere Client, where activity is subject to role-based access control and modern access control methods.

If you want to use an authorized SSH key, you can upload it. See ESXi SSH Keys.

Note: Access the host by using the vSphere Client, remote command-line tools (ESXCLI and PowerCLI), and published APIs. Do not enable remote access to the host using SSH unless special circumstances require that you enable SSH access.

1. Browse to the host in the inventory.
2. Click **Configure**, then click **Services** under System.
3. Manage ESXi, SSH, or Direct Console UI services.
   a) In the Services pane, select the service.
   b) Click **Edit Startup Policy** and select the startup policy **Start and stop manually**.
   c) To enable the service, click **Start**.

   When you select **Start and stop manually**, the service does not start when you reboot the host. If you want the service to start when you reboot the host, select **Start and stop with host**.

Set the availability and idle timeouts for the ESXi Shell. See Create a Timeout for ESXi Shell Availability and Create a Timeout for Idle ESXi Shell Sessions.

Related Links

Use the Direct Console User Interface to Enable Access to the ESXi Shell on page 2761
The Direct Console User Interface (DCUI) allows you to interact with the host locally using text-based menus. Evaluate carefully whether the security requirements of your environment support enabling the Direct Console User Interface.

Log in to the ESXi Shell for Troubleshooting on page 2763
Perform ESXi configuration tasks with the vSphere Client, ESXCLI, or VMware PowerCLI. Log in to the ESXi Shell (formerly Tech Support Mode or TSM) for troubleshooting purposes only.

Create a Timeout for ESXi Shell Availability

The ESXi Shell is disabled by default. You can set an availability timeout for the ESXi Shell to increase security when you enable the shell.

The availability timeout setting is the amount of time that can elapse before you must log in after the is enabled. After the timeout period, the service is disabled and users are not allowed to log in.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Advanced System Settings**.
4. Click **Edit**, and select `UserVars.ESXiShellTimeOut`.
5. Enter the idle timeout setting.
   You must restart the SSH service and the ESXi Shell service for the timeout to take effect.
6. Click **OK**.

If you are logged in when the timeout period elapses, your session will persist. However, after you log out or your session is terminated, users are not allowed to log in.

Create a Timeout for Idle ESXi Shell Sessions

If you enable the ESXi Shell on a host, but forget to log out of the session, the idle session remains connected indefinitely. The open connection increases the potential for someone to gain privileged access to the host. Prevent this by setting a timeout for idle sessions.

The idle timeout is the amount of time that can elapse before a user is logged out of an idle interactive session. You can control the amount of time for both local and remote (SSH) session from the Direct Console Interface (DCUI) or from the vSphere Client.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, select **Advanced System Settings**.
4. Click **Edit**, select `UserVars.ESXiShellInteractiveTimeOut`, and enter the timeout setting.
   A value of zero (0) disables the idle time.
5. Restart the ESXi Shell service and the SSH service for the timeout to take effect.

If the session is idle, users are logged out after the timeout period elapses.

Use the Direct Console User Interface to Enable Access to the ESXi Shell

The Direct Console User Interface (DCUI) allows you to interact with the host locally using text-based menus. Evaluate carefully whether the security requirements of your environment support enabling the Direct Console User Interface.

You can use the Direct Console User Interface (DCUI) to enable local and remote access to the ESXi Shell. You access the Direct Console User Interface from the physical console attached to the host. After the host reboots and loads ESXi, press F2 to log in to the DCUI. Enter the credentials that you created when you installed ESXi.

Note: Changes made to the host using the Direct Console User Interface, the vSphere Client, ESXCLI, or other administrative tools are committed to permanent storage every hour or upon graceful shutdown. If the host fails before the changes are committed, they might be lost.

1. From the Direct Console User Interface, press F2 to access the System Customization menu.
2. Select **Troubleshooting Options** and press Enter.
3. From the Troubleshooting Mode Options menu, select a service to enable.
   - Enable
   - Enable SSH
4. Press Enter to enable the service.
5. Press Esc until you return to the main menu of the Direct Console User Interface.

Set the availability and idle timeouts for the ESXi Shell. See Set Availability Timeout or Idle Timeout for the ESXi Shell.

Related Links

Enable Access to the ESXi Shell on page 2760

ESXi Shell and SSH interfaces are disabled by default. Keep these interfaces disabled unless you are performing troubleshooting or support activities. For day-to-day activities, use the vSphere Client, where activity is subject to role-based access control and modern access control methods.

Log in to the ESXi Shell for Troubleshooting on page 2763

Perform ESXi configuration tasks with the vSphere Client, ESXCLI, or VMware PowerCLI. Log in to the ESXi Shell (formerly Tech Support Mode or TSM) for troubleshooting purposes only.

Set Availability Timeout or Idle Timeout for the ESXi Shell

The ESXi Shell is disabled by default. To increase security when you enable the shell, you can set an availability timeout, an idle timeout, or both.

Enable the ESXi Shell. See Use the Direct Console User Interface to Enable Access to the ESXi Shell.

The two types of timeout apply in different situations.

Idle Timeout	If a user enables the ESXi Shell on a host, but forgets to log out of the session, the idle session remains connected indefinitely. The open connection can increase the potential for someone to gain privileged access to the host. You can prevent this situation by setting a timeout for idle sessions.
Availability Timeout	The availability timeout determines how much time can elapse before you log in after you initially enable the shell. If you wait longer, the service is disabled and you cannot log in to the ESXi Shell.

1. Log in to the ESXi Shell.
2. From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.
3. Enter the idle timeout (in seconds) or the availability timeout.
   You must restart the SSH service and the ESXi Shell service for the timeout to take effect.
4. Press Enter and press Esc until you return to the main menu of the Direct Console User Interface.
5. Click **OK**.

- If you set the idle timeout, users are logged out after the session is idle for the specified time.
- If you set the availability timeout, and you do not log in before that timeout elapses, logins become disabled again.

Log in to the ESXi Shell for Troubleshooting

Perform ESXi configuration tasks with the vSphere Client, ESXCLI, or VMware PowerCLI. Log in to the ESXi Shell (formerly Tech Support Mode or TSM) for troubleshooting purposes only.

1. Log in to the ESXi Shell using one of the following methods.
   - If you have direct access to the host, press Alt+F1 to open the login page on the machine's physical console.
   - If you are connecting to the host remotely, use SSH or another remote console connection to start a session on the host.
2. Enter a user name and password recognized by the host.

Related Links

Enable Access to the ESXi Shell on page 2760

ESXi Shell and SSH interfaces are disabled by default. Keep these interfaces disabled unless you are performing troubleshooting or support activities. For day-to-day activities, use the vSphere Client, where activity is subject to role-based access control and modern access control methods.

Use the Direct Console User Interface to Enable Access to the ESXi Shell on page 2761

The Direct Console User Interface (DCUI) allows you to interact with the host locally using text-based menus. Evaluate carefully whether the security requirements of your environment support enabling the Direct Console User Interface.

UEFI Secure Boot for ESXi Hosts

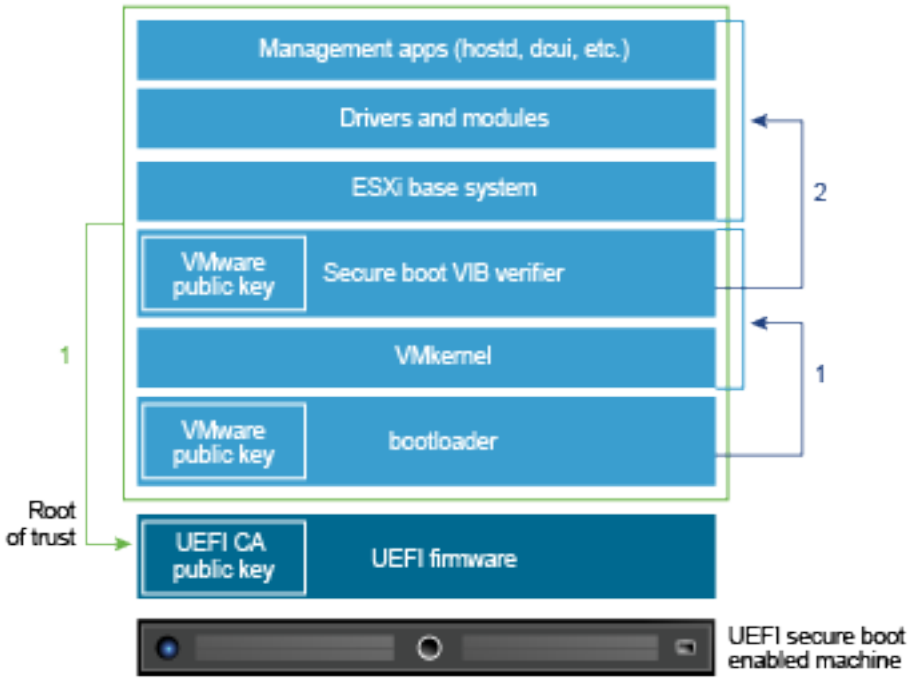
Secure boot is part of the UEFI firmware standard. With secure boot enabled, a machine refuses to load any UEFI driver or app unless the operating system bootloader is cryptographically signed. Starting with vSphere 6.5, ESXi supports secure boot if it is enabled in the hardware.

How ESXi Uses UEFI Secure Boot

ESXi version 6.5 and later supports UEFI Secure Boot at each level of the boot stack.

Note: Before you use UEFI Secure Boot on a host that was upgraded, check for compatibility by following the instructions in Run the Secure Boot Validation Script on an Upgraded ESXi Host.

Figure 89: UEFI Secure Boot



With secure boot enabled, the boot sequence proceeds as follows.

1. Starting with vSphere 6.5, the ESXi bootloader contains a VMware public key. The bootloader uses this key to verify the signature of the kernel and a small subset of the system that includes a secure boot VIB verifier.
2. The VIB verifier verifies every VIB package that is installed on the system.

At this point, the entire system boots with the root of trust in certificates that are part of the UEFI firmware.

Note: When you install or upgrade to vSphere 7.0 Update 2 or later, and an ESXi host has a TPM, the TPM seals the sensitive information by using a TPM policy based on PCR values for UEFI Secure Boot. This value is loaded during subsequent reboots if the policy is satisfied as true. To disable or enable UEFI Secure Boot in vSphere 7.0 Update 2 and later, see Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration.

Troubleshooting UEFI Secure Boot

If secure boot does not succeed at any level of the boot sequence, an error results.

The error message depends on the hardware vendor and on the level at which verification did not succeed.

- If you attempt to boot with a bootloader that is unsigned or has been tampered with, an error during the boot sequence results. The exact message depends on the hardware vendor. It might look like the following error, but might look different.

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- If the kernel has been tampered with, an error like the following results.

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- If a package (VIB or driver) has been tampered with, a purple screen with the following message appears.

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

To resolve issues with secure boot, follow these steps.

1. Reboot the host with secure boot disabled.

2. Run the secure boot verification script (see Run the Secure Boot Validation Script on an Upgraded ESXi Host).
3. Examine the information in the `/var/log/esxupdate.log` file.

Securing ESXi Hosts with Trusted Platform Module

ESXi hosts can use Trusted Platform Modules (TPM) chips, which are secure cryptoprocessors that enhance host security by providing a trust assurance rooted in hardware as opposed to software.

TPM is an industry-wide standard for secure cryptoprocessors. TPM chips are found in most of today's computers, from laptops, to desktops, to servers. vSphere 6.7 and later supports TPM version 2.0.

A TPM 2.0 chip attests to an ESXi host's identity. Host attestation is the process of authenticating and attesting to the state of the host's software at a given point in time. UEFI secure boot, which ensures that only signed software is loaded at boot time, is a requirement for successful attestation. The TPM 2.0 chip records and securely stores measurements of the software modules booted in the system, which vCenter Server remotely verifies.

The high-level steps of the remote attestation process are:

1. Establish the trustworthiness of the remote TPM and create an Attestation Key (AK) on it.
   When an ESXi host is added to, rebooted from, or reconnected to vCenter Server, vCenter Server requests an AK from the host. Part of the AK creation process also involves the verification of the TPM hardware itself, to ensure that a known (and trusted) vendor has produced it.
2. Retrieve the Attestation Report from the host.
   vCenter Server requests that the host sends an Attestation Report, which contains a quote of Platform Configuration Registers (PCRs), signed by the TPM, and other signed host binary metadata. By checking that the information corresponds to a configuration it deems trusted, a vCenter Server identifies the platform on a previously untrusted host.
3. Verify the host's authenticity.
   vCenter Server verifies the authenticity of the signed quote, infers the software versions, and determines the trustworthiness of said software versions. If vCenter Server determines the signed quote is invalid, remote attestation fails and the host is not trusted.

To use a TPM 2.0 chip, your vCenter Server environment must meet these requirements:

- vCenter Server 6.7 or later
- ESXi 6.7 host or later with TPM 2.0 chip installed and enabled in UEFI
- UEFI Secure Boot enabled

Ensure that the TPM is configured in the ESXi host's BIOS to use the SHA-256 hashing algorithm and the TIS/FIFO (First-In, First-Out) interface and not CRB (Command Response Buffer). For information about setting these required BIOS options, refer to the vendor documentation.

Review the TPM 2.0 chips certified by VMware at the following location:

https://www.vmware.com/resources/compatibility/search.php

When you boot an ESXi host with an installed TPM 2.0 chip, vCenter Server monitors the host's attestation status. The vSphere Client displays the hardware trust status in the vCenter Server's **Summary** tab under **Security** with the following alarms:

- Green: Normal status, indicating full trust.
- Red: Attestation failed.

Note: If you add a TPM 2.0 chip to an ESXi host that vCenter Server already manages, you must first disconnect the host, then reconnect it. See *vCenter Server and Host Management* documentation for information about disconnecting and reconnecting hosts.

View ESXi Host Attestation Status

When added to an ESXi host, a Trusted Platform Module 2.0 compatible chip attests the integrity of the platform. You can view the attestation status of the host in the vSphere Client. You can also view the Intel Trusted Execution Technology (TXT) status.

1. Connect to vCenter Server by using the vSphere Client.
2. Navigate to a data center and click the **Monitor** tab.
3. Click **Security**.
4. Review the host's status in the Attestation column and read the accompanying message in the **Message** column.
5. If this host is a Trusted Host, see View the Trusted Cluster Attestation Status for more information.

For a Failed or Warning attestation status, see Troubleshoot ESXi Host Attestation Problems. For Trusted Hosts, see Troubleshoot Trusted Host Attestation Problems.

Troubleshoot ESXi Host Attestation Problems

When you install a Trusted Platform Module (TPM) device on an ESXi host, the host might fail to pass attestation. You can troubleshoot the potential causes of this problem.

1. View the ESXi host alarm status and accompanying error message. See View ESXi Host Attestation Status.
2. If the error message is `Host secure boot was disabled`, you must re-enable secure boot to resolve the problem.
3. If the attestation status of the host is failed, check the vCenter Server`vpxd.log` file for the following message:

   `No cached identity key, loading from DB`

   This message indicates that you are adding a TPM 2.0 chip to an ESXi host that vCenter Server already manages. You must first disconnect the host, then reconnect it. See *vCenter Server and Host Management* documentation for information about disconnecting and reconnecting hosts.

   For more information about vCenter Server log files, including location and log rotation, see the VMware knowledge base article at https://kb.vmware.com/s/article/1021804.
4. For all other error messages, contact Customer Support.

ESXi Log Files

Log files are an important component of troubleshooting attacks and obtaining information about breaches. Logging to a secure, centralized log server can help prevent log tampering. Remote logging also provides a long-term audit record.

To increase the security of the host, take the following measures.

- Configure persistent logging to a datastore. By default, the logs on ESXi hosts are stored in the in-memory file system. Therefore, they are lost when you reboot the host, and only 24 hours of log data is stored. When you enable persistent logging, you have a dedicated activity record for the host.
- Remote logging to a central host allows you to gather log files on a central host. From that host, you can monitor all hosts with a single tool, do aggregate analysis, and search log data. This approach facilitates monitoring and reveals information about coordinated attacks on multiple hosts.
- Configure the remote secure syslog on ESXi hosts by using ESXCLI or PowerCLI, or by using an API client.
- Query the syslog configuration to make sure that the syslog server and port are valid.

See the *vSphere Monitoring and Performance* documentation for information about syslog setup, and for additional information on ESXi log files.

Configure Syslog on ESXi Hosts

You can use the vSphere Client, the VMware Host Client, or the `esxcli system syslog` command to configure the syslog service.

The syslog service receives, categorizes, and stores log messages for analyses that help you take preventive action in your environment.

ESXi Log File Locations

ESXi records host activity in log files, using a syslog facility.

Table 244: ESXi Log File Locations

Component	Location	Purpose
Authentication	`/var/log/auth.log`	Contains all events related to authentication for the local system.
ESXi host agent log	`/var/log/hostd.log`	Contains information about the agent that manages and configures the ESXi host and its virtual machines.
Shell log	`/var/log/shell.log`	Contains a record of all commands typed into the ESXi Shell and shell events (for example, when the shell was enabled).
System messages	`/var/log/syslog.log`	Contains all general log messages and can be used for troubleshooting. This information was formerly located in the messages log file.
vCenter Server agent log	`/var/log/vpxa.log`	Contains information about the agent that communicates with vCenter Server (if the host is managed by vCenter Server).
Virtual machines	The same directory as the affected virtual machine's configuration files, named `vmware.log` and `vmware*.log`. For example, `/vmfs/volumes/datastore/virtual machine/vmware.log`	Contains virtual machine power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, machine clones, and so on.
VMkernel	`/var/log/vmkernel.log`	Records activities related to virtual machines and ESXi.
VMkernel summary	`/var/log/vmksummary.log`	Used to determine uptime and availability statistics for ESXi (comma separated).
VMkernel warnings	`/var/log/vmkwarning.log`	Records activities related to virtual machines.
Quick Boot	`/var/log/loadESX.log`	Contains all events related to restarting an ESXi host through Quick Boot.
Trusted infrastructure agent	`/var/run/log/kmxa.log`	Records activities related to the Client Service on the ESXi Trusted Host.
Key Provider Service	`/var/run/log/kmxd.log`	Records activities related to the vSphere Trust Authority Key Provider Service.
Attestation Service	`/var/run/log/attestd.log`	Records activities related to the vSphere Trust Authority Attestation Service.

Component	Location	Purpose
ESX Token Service	`/var/run/log/esxtokend.log`	Records activities related to the vSphere Trust Authority ESX Token Service.
ESX API Forwarder	`/var/run/log/esxapiadapter.log`	Records activities related to the vSphere Trust Authority API forwarder.

Securing Fault Tolerance Logging Traffic

VMware Fault Tolerance (FT) captures inputs and events that occur on a primary VM and sends them to the secondary VM, which is running on another host.

This logging traffic between the primary and secondary VMs is unencrypted and contains guest network and storage I/O data, as well as the memory contents of the guest operating system. This traffic might include sensitive data such as passwords in plaintext. To avoid such data being divulged, ensure that this network is secured, especially to avoid man-in-the-middle attacks. For example, use a private network for FT logging traffic.

Activate Fault Tolerance Encryption

You can encrypt Fault Tolerance log traffic.

FT encryption requires SMP-FT. Encryption on Legacy FT (Record-Replay FT) is not supported.

vSphere Fault Tolerance performs frequent checks between a primary VM and secondary VM so that the secondary VM can quickly resume from the last successful checkpoint. The checkpoint contains the VM state that has been modified since the previous checkpoint. You can encrypt Fault Tolerance log traffic.

When you turn on Fault Tolerance, FT encryption is set to **Opportunistic** by default, which means it activates encryption only if both the primary and secondary host are capable of encryption. Follow this procedure if you need to change the FT encryption mode manually.

Note: Fault Tolerance supports vSphere Virtual Machine Encryption with vSphere 7.0 Update 2 and later. In-guest and array-based encryption do not depend on or interfere with VM encryption. Having multiple encryption layers uses additional compute resources, which might impact virtual machine performance. The impact varies with hardware as well as the amount and type of I/O, but overall performance impact is negligible for most workloads. The effectiveness and compatibility of back-end storage features such as deduplication, compression, and replication might also be affected by VM encryption.

1. Select the VM and choose **Edit Settings**.
2. Under **VM Options** select the **Encrypted FT** drop-down menu.
3. Choose one of the following options:

Option	Description
Disabled	Do not turn on encrypted Fault Tolerance logging.
Opportunistic	Turn on encryption only if both sides are capable. A Fault Tolerance VM is allowed to move to an ESXi host which does not support encrypted Fault Tolerance logging.
Required	Choose hosts for Fault Tolerance primary and secondary that both support encrypted FT logging.

Note: While VM encryption is activated, FT encryption mode is set to **Required** by default and cannot be modified.

When FT encryption mode is set to **Required**:

- When you turn on FT, only FT encryption supported hosts are listed for the placement of FT secondary.
- FT failover can only happen on the FT encryption supported hosts.

4. Click **OK**.

Managing ESXi Audit Records

Audit records conform to RFC 5424 and contain information about events pertaining to items such as the time, status, description, and user information logged for events that have occurred from actions on ESXi hosts. Both local and remote audit record keeping are available. Audit record keeping is deactivated by default. You must manually activate both local and remote auditing modes.

Audit records, when enabled, are stored locally as a fixed-size buffer of recent additions. Once the audit records fill the buffer, new audit records overwrite the oldest records.

Audit records are stored in RFC 5424 format but are transmitted to remote hosts in compliance with the specified message formatting (RFC 3164 for ESXi 7.0 Update 3). The audit records are part of the stream of syslog messages. You can configure the local storage and transmission of audit records independently of each other. When you activate both local storage and transmission, the audit records are stored and transmitted simultaneously.

During a loss of connection between the ESXi host transmitting syslog data and a remote host, audit records are dropped if the available buffer space is exceeded. Upon reconnection, the system generates an audit message indicating potential message loss.

Configuring Audit Records

You use ESXCLI to configure the local audit record keeping. For more information, see *ESXCLI Reference* at https://code.vmware.com/.

Viewing Audit Records

You can view the audit records as follows.

- Local: Use the ESXi `/bin/viewAudit` application.
- Remote: Configure a remote audit server using ESXCLI. For more information, see see Enable the Transmission of Audit Records to a Remote Host with ESXCLI.

You can also use the FetchAuditRecords API (in the DiagnosticsManager managed object) to view audit records.

Securing the ESXi Configuration

Starting in vSphere 7.0 Update 2, the ESXi configuration is protected by encryption. When an ESXi host is optionally protected by a TPM, the ESXi configuration encryption key is sealed by the TPM.

Many ESXi services store secrets in their configuration files. These configurations persist in an ESXi host's boot bank as an archived file. Beginning in vSphere 7.0 Update 2, this archived file is encrypted. As a result, attackers cannot read or alter this file directly, even if they have physical access to the ESXi host's storage.

In addition to preventing an attacker from accessing secrets, a secure ESXi configuration when used with a TPM can save virtual machine encryption keys across reboots. As a result, encrypted workloads can continue to function when a key server is unavailable or unreachable. See Key Persistence Overview.

Securing the ESXi Configuration Overview

You do not need to enable ESXi configuration encryption manually. When you install or upgrade to vSphere 7.0 Update 2 or later, the archived ESXi configuration file is encrypted.

Before vSphere 7.0 Update 2, the archived ESXi configuration file is not encrypted. In vSphere 7.0 Update 2 and later, the archived configuration file is encrypted. When the ESXi host is configured with a Trusted Platform Module (TPM), the TPM is used to "seal" the configuration to the host, providing a strong security guarantee.

ESXi Configuration Files Overview before vSphere 7.0 Update 2

The configuration of an ESXi host consists of configuration files for each service that runs on the host. The configuration files typically reside in the `/etc/` directory, but they can also reside in other namespaces. The configuration files contain run-time information about the state of the services. Over time, the default values in the configuration files can change, for example, when you change settings on the ESXi host. A cron job backs up the ESXi configuration files periodically, or when ESXi shuts down gracefully, or on demand, and creates an archived configuration file in the boot bank. When ESXi reboots, it reads the archived configuration file and recreates the state that ESXi was in when the backup was taken. Before vSphere 7.0 Update 2, the archived configuration file is unencrypted. As a result, it is possible for an attacker who has access to the physical ESXi storage to read and alter this file while the system is offline.

Secure ESXi Configuration Overview

During the first boot after installing or upgrading the ESXi host to vSphere 7.0 Update 2 or later, the following occurs:

- If the ESXi host has a TPM, and it is enabled in the firmware, the archived configuration file is encrypted by an encryption key stored in the TPM. From this point on, the configuration of the host is sealed by the TPM.
- If the ESXi host does not have a TPM, ESXi uses a Key Derivation Function (KDF) to generate a secure configuration encryption key for the archived configuration file. The inputs to the KDF are stored on disk in the `encryption.info` file.

Note: When an ESXi host has an enabled TPM device, you gain additional protection.

When the ESXi host reboots after the first boot, the following occurs:

- If the ESXi host has a TPM, the host must obtain the encryption key from the TPM for that specific host. If the TPM measurements satisfy the sealing policy that was used when creating the encryption key, then the host obtains the encryption key from the TPM.
- If the ESXi host does not have a TPM, ESXi reads information from the `encryption.info` file to unlock the secure configuration.

Secure ESXi Configuration Requirements

- ESXi 7.0 Update 2 or later
- TPM 2.0 for configuration encryption and ability to use a sealing policy

Secure ESXi Configuration Recovery Key

A secure ESXi configuration includes a recovery key. If you must recover the ESXi secure configuration, you use a recovery key whose contents you enter as a command-line boot option. You can list the recovery key to create a recovery key backup. You can also rotate the recovery key as part of your security requirements.

Taking a backup of the recovery key is an important part of managing your secure ESXi configuration. vCenter Server generates an alarm to remind you to back up the recovery key.

Recovery Key Alarm

Taking a backup of the recovery key is an important part of managing your secure ESXi configuration. Whenever an ESXi host in TPM mode is connected or reconnected to vCenter Server, vCenter Server generates an alarm to remind you to back up the recovery key. When you reset the alarm, it is not triggered again unless conditions change.

Best Practices for Secure ESXi Configuration

Follow these best practices for the recovery key:

- When you list a recovery key, it is temporarily displayed in an untrusted environment and is in memory. Remove traces of the key.
  - Rebooting the host removes the residual key in memory.
  - For enhanced protection, you can enable encryption mode on the host. See Enable Host Encryption Mode Explicitly.
- When you perform a recovery:
  - To eliminate any traces of the recovery key in an untrusted environment, reboot the host.
  - For enhanced security, rotate the recovery key to use a new key after having recovered the key one time.

TPM Sealing Policies Overview

In vSphere 7.0 Update 2 and later, an ESXi host uses the TPM to seal the host's configuration against a Platform Configuration Register (PCR) policy. The PCR policy can be configured to enforce UEFI Secure Boot and other settings.

A TPM can use Platform Configuration Register (PCR) measurements to implement policies that restrict unauthorized access to sensitive data. When you install or upgrade an ESXi host with a TPM to vSphere 7.0 Update 2 and later, the TPM seals the sensitive information by using a policy that incorporates the secure boot setting. This policy checks that if secure boot was enabled when data was first sealed with the TPM, then secure boot must still be enabled when attempting to unseal the data on a subsequent boot.

Secure boot is part of the UEFI firmware standard. With UEFI Secure Boot enabled, a host refuses to load any UEFI driver or app unless the operating system bootloader has a valid digital signature.

You can choose to disable or enable UEFI Secure Boot enforcement. See Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration.

Note: If you do not activate a TPM when you install or upgrade to vSphere 7.0 Update 2 or later, you can do so later with the following command.

```
esxcli system settings encryption set --mode=TPM
```

Once you have activated the TPM, you cannot undo the setting.

The `esxcli system settings encryption set` command fails on some TPMs even when the TPM is enabled for the host.

- In vSphere 7.0 Update 2: TPMs from NationZ (NTZ), Infineon Technologies (IFX), and certain new models (like NPCT75x) from Nuvoton Technologies Corporation (NTC)
- In vSphere 7.0 Update 3: TPMs from NationZ (NTZ)

If an installation or upgrade of vSphere 7.0 Update 2 or later is unable to use the TPM during the first boot, the installation or upgrade continues, and the mode defaults to NONE (that is, `--mode=NONE`). The resulting behavior is as though the TPM is not activated.

The TPM can also enforce the setting for the execInstalledOnly boot option in the sealing policy. The execInstalledOnly enforcement is an advanced ESXi boot option that guarantees that the VMkernel executes only binaries that have been properly packaged and signed as part of a VIB. The execInstalledOnly boot option has a dependency on the secure boot option. The secure boot enforcement must be enabled before you can enforce the execInstalledOnly boot option in the sealing policy. See Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration.

Managing a Secure ESXi Configuration

You can use ESXCLI commands to list the secure ESXi configuration recovery key, rotate the recovery key, and change the TPM policies (for example, enforcing UEFI Secure Boot).

List the Contents of the Secure ESXi Configuration Recovery Key

You can use ESXCLI to show the contents of the secure ESXi configuration recovery key.

- Have access to the ESXCLI command set. You can run ESXCLI commands remotely, or run them in the ESXi Shell.
- Required privilege for using ESXCLI standalone version or through PowerCLI: **Host** > **Config** > **Settings**

This task applies only to an ESXi host that has a TPM. In general, you list the contents of the secure ESXi configuration recovery key to create a backup, or as part of rotating recovery keys.

1. Run the following command on the ESXi host.

   ```
   esxcli system settings encryption recovery list
   ```

2. Save the output in a secure, remote location as a backup, in case you must recover the secure configuration.

The recovery key ID and key are displayed.

List the Secure ESXi Configuration Recovery Key

```
[root@host1] esxcli system settings encryption recovery list

Recovery ID                             Key
--------------------------------------  ---
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}
 478269-039194-473926-430939-686855-231401-642208-184477-602511
-225586-551660-586542-338394-092578-687140-267425
```

Rotate the Secure ESXi Configuration Recovery Key

You can use ESXCLI to rotate the secure ESXi configuration recovery key.

- Have access to the ESXCLI command set. You can run ESXCLI commands remotely, or run them in the ESXi Shell.
- Required privilege for using ESXCLI standalone version or through PowerCLI: **Host** > **Config** > **Settings**

This task applies only to an ESXi host that has a TPM. You can rotate the ESXi secure configuration recovery key as part of your security best practices.

1. List the recovery key.

   See List the Contents of the Secure ESXi Configuration Recovery Key.

2. Run the following command.

   ```
   esxcli system settings encryption recovery rotate [-k keyID] -u uuid
   ```

   In this command, the optional *keyID* is the key ID in the VMkernel key cache and *uuid* is the Recovery ID (obtained from the `esxcli system settings encryption recovery list` command). If you do not supply the optional key ID, ESXi replaces the old recovery key with a new recovery key that is randomly generated.

The recovery key is now set to the contents of the key referenced by key ID, if provided. Otherwise, ESXi provides a new key ID.

Troubleshooting and Recovering the Secure ESXi Configuration

You can troubleshoot and recover from boot problems that you might encounter with a secure ESXi Configuration.

If you clear a TPM (that is, the seed values in the TPM are reset), if a TPM fails, or if you replace the motherboard or TPM device, or both, you must take steps to recover the ESXi secure configuration. You must have the recovery key to recover the configuration. Until you recover the configuration, the ESXi host cannot boot. See Recover the Secure ESXi Configuration.

Although uncommon, it is possible that an ESXi host might fail to restore or decrypt the secure configuration, preventing the host from booting. Possible situations include:

- Change to secure boot setting (or other policy)

- Actual tampering
- The recovery key is unavailable

To troubleshoot these conditions, see the VMware knowledge base article at https://kb.vmware.com/kb/81446.

Recover the Secure ESXi Configuration

If a TPM fails, or if you clear a TPM, you must recover the secure ESXi Configuration. Until you recover the configuration, the ESXi host cannot boot.

Get your recovery key. You should have previously listed and stored the recover key. See List the Contents of the Secure ESXi Configuration Recovery Key.

Recovering the secure ESXi configuration refers to the following situations:

- You cleared the TPM (that is, the seeds in the TPM were reset).
- The TPM failed.
- You replaced the motherboard or the TPM device, or both.

To troubleshoot other secure ESXi configuration problems, see the VMware knowledge base article at https://kb.vmware.com/kb/81446.

Perform the recovery manually. Do not perform the recovery as part of an installation or upgrade script.

1. Optional: If the TPM failed, move the disk (having the boot bank) to another host with a TPM.
2. Start the ESXi host.
3. When the ESXi installer window appears, press Shift+O to edit boot options.
4. To recover the configuration, at the command prompt, append the following boot option to any existing boot options.

   ```
   encryptionRecoveryKey=recovery_key
   ```

   The secure ESXi configuration is recovered and the ESXi host boots.
5. To persist the change, enter the following command:

   ```
   /sbin/auto-backup.sh
   ```

When you enter the recovery key, it is temporarily displayed in an untrusted environment and is in memory. Though not necessary, as a best practice, you can remove residual traces of the key in memory by rebooting the host. Or, you can rotate the key. See Rotate the Secure ESXi Configuration Recovery Key.

Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration

You can choose to enable UEFI secure boot enforcement, or disable a previously enabled UEFI secure boot enforcement. You must use ESXCLI to change the setting in the TPM on the ESXi host.

- Have access to the ESXCLI command set. You can run ESXCLI commands remotely, or run them in the ESXi Shell.
- Required privilege for using ESXCLI standalone version or through PowerCLI: **Host** > **Config** > **Settings**

This task applies only to ESXi hosts that have a TPM. UEFI Secure boot is a firmware setting for ensuring that the software launched by the firmware is trusted. To learn more, see UEFI Secure Boot for ESXi Hosts. The enablement of UEFI Secure boot can be enforced upon every boot by using the TPM.

1. List the current settings on the ESXi host.

   ```
   esxcli system settings encryption get
      Mode: TPM
      Require Executables Only From Installed VIBs: false
      Require Secure Boot: true
   ```

If secure boot enforcement is enabled, Require Secure Boot displays true. If secure boot enforcement is disabled, Require Secure Boot displays false.

If Mode appears as NONE, you must enable the TPM in the host's firmware and set the mode by running the following command:

```
esxcli system settings encryption set --mode=TPM
```

2. Enable or disable the secure boot enforcement.

Option	Description

Enable	1. Shut down the host gracefully.
	For example, right-click the ESXi host in the vSphere Client and select **Power** > **Shut Down**.
	2. Enable secure boot in the firmware of the host.
	See your specific vendor hardware documentation.
	3. Restart the host.
	4. Run the following ESXCLI command.
	`esxcli system settings encryption set --require-secure-boot=T`
	5. Verify the change.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Confirm that Required Secure Boot displays true.
	6. To save the setting, run the following command.
	`/bin/backup.sh 0`

Disable	1. Run the following ESXCLI command.
	`esxcli system settings encryption set --require-secure-boot=F`
	2. Verify the change.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: false`
	Confirm that Require Secure Boot displays false.
	3. To save the setting, run the following command.
	`/bin/backup.sh 0`
	You can choose to disable the secure boot in the firmware of the host, but at this point the dependency between the firmware setting and the TPM enforcement is no longer set.

The ESXi host runs with secure boot enforcement enabled or disabled, depending on your choice.

Note:

If you do not activate a TPM when you install or upgrade to vSphere 7.0 Update 2 or later, you can do so later with the following command.

```
esxcli system settings encryption set --mode=TPM
```

Once you have activated the TPM, you cannot undo the setting.

The `esxcli system settings encryption set` command fails on some TPMs even when the TPM is enabled for the host.

- In vSphere 7.0 Update 2: TPMs from NationZ (NTZ), Infineon Technologies (IFX), and certain new models (like NPCT75x) from Nuvoton Technologies Corporation (NTC)
- In vSphere 7.0 Update 3: TPMs from NationZ (NTZ)

If an installation or upgrade of vSphere 7.0 Update 2 or later is unable to use the TPM during the first boot, the installation or upgrade continues, and the mode defaults to NONE (that is, `--mode=NONE`). The resulting behavior is as though the TPM is not activated.

Enable or Disable the execInstalledOnly Enforcement for a Secure ESXi Configuration

You can choose to enable execInstalledOnly enforcement, or disable a previously enabled execInstalledOnly enforcement. You must use ESXCLI to change the setting in the TPM on the ESXi host. UEFI secure boot enforcement must be enabled before you can enable the execInstalledOnly enforcement.

- To enable the execInstalledOnly enforcement, you must first enable the UEFI secure boot enforcement. The execInstalledOnly enforcement is built on top of the UEFI secure boot enforcement. See Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration.
- Have access to the ESXCLI command set. You can run ESXCLI commands remotely, or run them in the ESXi Shell.
- Required privilege for using ESXCLI standalone version or through PowerCLI: **Host** > **Config** > **Settings**

This task applies only to ESXi hosts that have a TPM. The execInstalledOnly advanced ESXi boot option, when set to TRUE, guarantees that the VMkernel executes only those binaries that have been packaged and signed as part of a VIB. The enablement of this boot option can be enforced upon every boot by using the TPM.

1. List the current settings on the ESXi host.

   ```
   esxcli system settings encryption get
      Mode: TPM
      Require Executables Only From Installed VIBs: false
      Require Secure Boot: true
   ```

   If execInstalledOnly enforcement is enabled, Require Executables Only From Installed VIBs displays true. If execInstalledOnly enforcement is disabled, Require Executables Only From Installed VIBs displays false. To enable the execInstalledOnly enforcement, the secure boot enforcement must be enabled, and Require Secure Boot displays true in this case.

   If Mode appears as NONE, you must enable the TPM in the host's firmware and set the mode by running the following command:

   ```
   esxcli system settings encryption set --mode=TPM
   ```

   Also, if Require Secure Boot displays as False, see Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration to enable the enforcement.

2. Enable or disable the execInstalledOnly enforcement.

Option	Description

Enable	1. Verify that the secure boot option is enforced.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Confirm that Require Secure Boot displays true. If not, see Enable or Disable the Secure Boot Enforcement for a Secure ESXi Configuration.

Option	Description

	2. To configure the runtime value of the execInstalledOnly boot option to TRUE, run the following ESXCLI command.
	`esxcli system settings kernel set -s execInstalledOnly -v TRUE`
	3. Shut down the host gracefully.
	For example, right-click the ESXi host in the vSphere Client and select **Power** > **Shut Down**.
	4. Restart the host.
	5. To set the execInstalledOnly enforcement, run the following ESXCLI command.
	`esxcli system settings encryption set --require-exec-installed-only=T`
	6. Verify the change.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: true`
	`Require Secure Boot: true`
	Confirm that Require Executables Only From Installed VIBs displays true.
	7. To save the setting, run the following command.
	`/bin/backup.sh 0`

Disable	1. Run the following ESXCLI command.
	`esxcli system settings encryption set --require-exec-installed-only=F`
	2. Verify the change.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Confirm that Require Executables Only From Installed VIBs displays false.
	3. To save the setting, run the following command.
	`/bin/backup.sh 0`
	The TPM no longer enforces the execInstalledOnly boot option.

The ESXi host runs with execInstalledOnly enforcement enabled or disabled, depending on your choice.

Securing vCenter Server Systems

Securing vCenter Server includes ensuring security of the host where vCenter Server is running, following best practices for assigning privileges and roles, and verifying the integrity of the clients that connect to vCenter Server.

vCenter Server Security Best Practices

Following vCenter Server security best practices helps you ensure the integrity of your vSphere environment.

Best Practices for vCenter Server Access Control

Strictly control access to different vCenter Server components to increase security for the system.

The following guidelines help ensure security of your environment.

Use Named Accounts

- Grant the Administrator role only to those administrators who are required to have it. You can create custom roles or use the No cryptography administrator role for administrators with more limited privileges. Do not apply this role to any group whose membership is not strictly controlled.
- Make sure that applications use unique service accounts when connecting to a vCenter Server system.

Monitor Privileges of vCenter Server Administrator Users

Not all administrator users must have the Administrator role. Instead, create a custom role with the appropriate set of privileges and assign it to other administrators.

Users with the vCenter Server Administrator role have privileges on all objects in the hierarchy. For example, by default the Administrator role allows users to interact with files and programs inside a virtual machine's guest operating system. Assigning that role to too many users can lessen virtual machine data confidentiality, availability, or integrity. Create a role that gives the administrators the privileges they need, but remove some of the virtual machine management privileges.

Minimize Access

Do not allow users to log directly in to the vCenter Server host machine. Users who are logged in to the vCenter Server host machine can cause harm, either intentionally or unintentionally, by altering settings and modifying processes. Those users also have potential access to vCenter credentials, such as the SSL certificate. Allow only users who have legitimate tasks to perform to log in to the system and ensure that login events are audited.

Grant Minimal Privileges to vCenter Server Database Users

The database user requires only certain privileges specific to database access.

Some privileges are required only for installation and upgrade. You can remove these privileges from the database administrator after vCenter Server is installed or upgraded.

Restrict Datastore Browser Access

Assign the **Datastore** > **Browse datastore** privilege only to users or groups who really need those privileges. Users with the privilege can view, upload, or download files on datastores associated with the vSphere deployment through the Web browser or the vSphere Client.

Restrict Users From Running Commands in a Virtual Machine

By default, a user with the vCenter Server Administrator role can interact with files and programs within a virtual machine's guest operating system. To reduce the risk of breaching guest confidentiality, availability, or integrity, create a custom nonguest access role without the **Guest Operations** privilege. See Restrict Users from Running Commands Within a Virtual Machine.

Consider Modifying the Password Policy for vpxuser

By default, vCenter Server changes the vpxuser password automatically every 30 days. Ensure that this setting meets company policy, or configure the vCenter Server password policy. See Set the vCenter Server Password Policy.

Note: Make sure that password aging policy is not too short.

Check Privileges After vCenter Server Restart

Check for privilege reassignment when you restart vCenter Server. If the user or group that has the Administrator role on the root folder cannot be validated during a restart, the role is removed from that user or group. In its place, vCenter Server grants the Administrator role to the vCenter Single Sign-On administrator, administrator@vsphere.local by default. This account can then act as the vCenter Server administrator.

Reestablish a named administrator account and assign the Administrator role to that account to avoid using the anonymous vCenter Single Sign-On administrator account (administrator@vsphere.local by default).

Use High RDP Encryption Levels

On each Windows computer in the infrastructure, ensure that Remote Desktop Host Configuration settings are set to ensure the highest level of encryption appropriate for your environment.

Verify vSphere Client Certificates

Instruct users of the vSphere Client or other client applications to heed certificate verification warnings. Without certificate verification, the user might be subject of a MiTM attack.

Set the vCenter Server Password Policy

By default, vCenter Server changes the vpxuser password automatically every 30 days. You can change that value from the vSphere Client.

1. Log in to the vCenter Server system by using the vSphere Client.
2. Select the vCenter Server system in the object hierarchy.
3. Click **Configure**.
4. Click **Advanced Settings** and click **Edit Settings**.
5. Click the **Filter** icon and enter `VimPasswordExpirationInDays`.
6. Set `VirtualCenter.VimPasswordExpirationInDays` to comply with your requirements.

Removing Expired or Revoked Certificates and Logs from Failed Installations

Leaving expired or revoked certificates or leaving vCenter Server installation logs for failed installation on your vCenter Server system can compromise your environment.

Removing expired or revoked certificates is required for the following reasons.

- If expired or revoked certificates are not removed from the vCenter Server system, the environment can be subject to a MiTM attack
- In certain cases, a log file that contains the database password in plain text is created on the system if vCenter Server installation fails. An attacker who breaks into the vCenter Server system, might gain access to this password and, at the same time, access to the vCenter Server database.

Limiting vCenter Server Network Connectivity

For improved security, avoid putting the vCenter Server system on any network other than a management network, and ensure that vSphere management traffic is on a restricted network. By limiting network connectivity, you limit certain types of attack.

vCenter Server requires access to a management network only. Avoid putting the vCenter Server system on other networks such as your production network or storage network, or on any network with access to the Internet. vCenter Server does not need access to the network where vMotion operates.

vCenter Server requires network connectivity to the following systems.

- All ESXi hosts.
- The vCenter Server database.
- Other vCenter Server systems (if the vCenter Server systems are part of a common vCenter Single Sign-On domain for purposes of replicating tags, permissions, and so on).
- Systems that are authorized to run management clients. For example, the vSphere Client, a Windows system where you use the PowerCLI, or any other SDK-based client.
- Infrastructure services such as DNS, Active Directory, and PTP or NTP.
- Other systems that run components that are essential to functionality of the vCenter Server system.

Use the firewall on the vCenter Server. Include IP-based access restrictions so that only necessary components can communicate with the vCenter Server system.

Evaluate the Use of Linux Clients with CLIs and SDKs

Communications between client components and a vCenter Server system or ESXi hosts are protected by SSL-based encryption by default. Linux versions of these components do not perform certificate validation. Consider restricting the use of these clients.

To improve security, you can replace the VMCA-signed certificates on the vCenter Server system and on the ESXi hosts with certificates that are signed by an enterprise or third-party CA. However, certain communications with Linux clients might still be vulnerable to machine-in-the-middle attacks. The following components are vulnerable when they run on the Linux operating system.

- ESXCLI commands
- vSphere SDK for Perl scripts
- Programs that are written using the vSphere Web Services SDK

You can relax the restriction against using Linux clients if you enforce proper controls.

- Restrict management network access to authorized systems only.
- Use firewalls to ensure that only authorized hosts are allowed to access vCenter Server.
- Use bastion hosts (jump-box systems) to ensure that the Linux clients are behind the "jump."

Examine Client Plug-Ins

vSphere Client extensions run at the same privilege level as the user who is logged in. A malicious extension can masquerade as a useful plug-in and perform harmful operations such as stealing credentials or changing the system configuration. To increase security, use an installation that includes only authorized extensions from trusted sources.

You must have privileges to access the vCenter Single Sign-On service. These privileges differ from vCenter Server privileges.

A vCenter installation includes an extensibility framework for the vSphere Client. You can use this framework to extend the client with menu selections or toolbar icons. The extensions can provide access to vCenter add-on components or external, Web-based functionality.

Using the extensibility framework results in a risk of introducing unintended capabilities. For example, if an administrator installs a plug-in in an instance of the vSphere Client, the plug-in can run arbitrary commands with the privilege level of that administrator.

To protect against a potential compromise of your vSphere Client, examine all installed plug-ins periodically and make sure that each plug-in comes from a trusted source.

1. Log in to the vSphere Client as administrator@vsphere.local or a user with vCenter Single Sign-On privileges.
2. From the Home page, select **Administration**, then select **Client Plug-Ins** under **Solutions**.
3. Examine the list of client plug-ins.

vCenter Server Security Best Practices

Follow all best practices for securing a vCenter Server system. Additional steps help you make your vCenter Server more secure.

Configure PTP or NTP	Ensure that all systems use the same relative time source. This time source must be in sync with an agreed-upon time standard such as Coordinated Universal Time (UTC). Synchronized systems are essential for certificate validation. PTP and NTP also make it easier to track an intruder in log files. Incorrect time settings make it difficult to inspect and correlate log files to detect attacks, and make auditing inaccurate. See Synchronize the Time in vCenter Server with an NTP Server.
Restrict vCenter Server network access	Restrict access to components that are required to communicate with the vCenter Server. Blocking access from unnecessary systems reduces the potential for attacks on the operating system. For the list of all supported ports and protocols in VMware products, including vSphere and vSAN, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/. You can search ports by VMware product, create a customized list of ports, and print or save port lists.
Configure a Bastion Host	To help protect your assets, configure a bastion host (also called a jump box) to perform elevated administrative tasks. A bastion host is a special-purpose computer that hosts a minimal number of administrative applications. All other unnecessary services are removed. The host typically resides on the management network. A bastion host increases the protection of assets through restricting login to key individuals, requiring firewall rules to log in, and adding monitoring through auditing tools.

vCenter Password Requirements and Lockout Behavior

To manage your vSphere environment, you must be aware of the vCenter Single Sign-On password policy, of vCenter Server passwords, and of lockout behavior.

vCenter Single Sign-On Administrator Password

The password for the administrator of vCenter Single Sign-On, administrator@vsphere.local by default, is specified by the vCenter Single Sign-On password policy. By default, this password must meet the following requirements:

- At least eight characters
- At least one lowercase character
- At least one numeric character
- At least one special character

vCenter Server Passwords

In vCenter Server, password requirements are dictated by vCenter Single Sign-On or by the configured identity source, which can be Active Directory, OpenLDAP.

vCenter Single Sign-On Lockout Behavior

Users are locked out after a preset number of consecutive failed attempts. By default, users are locked out after five consecutive failed attempts in three minutes and a locked account is unlocked automatically after five minutes.

Verify Thumbprints for Legacy ESXi Hosts

In vSphere 6.0 and later, hosts are assigned VMCA certificates by default. If you change the certificate mode to thumbprint, you can continue to use thumbprint mode for legacy hosts. You can verify the thumbprints in the vSphere Client.

Note: Certificates are preserved across upgrades by default.

1. Browse to the vCenter Server in the vSphere Client inventory.
2. Click **Configure**.
3. Under **Settings**, click **General**.
4. Click **Edit**.
5. Click **SSL settings**.
6. If any of your ESXi 5.5 or earlier hosts require manual validation, compare the thumbprints listed for the hosts to the thumbprints in the host console.

   To obtain the host thumbprint, use the Direct Console User Interface (DCUI).

   a) Log in to the direct console and press F2 to access the System Customization menu.
   b) Select **View Support Information**.

      The host thumbprint appears in the column on the right.
7. If the thumbprint matches, select the **Verify** check box next to the host.

   Hosts that are not selected will be disconnected after you click **OK**.
8. Click **Save**.

Required Ports for vCenter Server

The vCenter Server system must be able to send data to every managed host and receive data from the vSphere Client. To enable migration and provisioning activities between managed hosts, the source and destination hosts must be able to receive data from each other through predetermined TCP and UDP ports.

vCenter Server is accessed through predetermined TCP and UDP ports. If you manage network components from outside a firewall, you might be required to reconfigure the firewall to allow access on the appropriate ports. For the list of all supported ports and protocols in vSphere, see the VMware Ports and Protocols Tool™ at https://ports.broadcom.com.

During installation, if a port is in use or is blocked using a denylist, the vCenter Server installer displays an error message. You must use another port number to proceed with the installation. There are internal ports that are used only for inter-process communication.

VMware uses designated ports for communication. Additionally, the managed hosts monitor designated ports for data from vCenter Server. If a built-in firewall exists between any of these elements, the installer opens the ports during the installation or upgrade process. For custom firewalls, you must manually open the required ports. If you have a firewall between two managed hosts and you want to perform source or target activities, such as migration or cloning, you must configure a means for the managed hosts to receive data.

To configure the vCenter Server system to use a different port to receive vSphere Client data, see the *vCenter Server and Host Management* documentation.

Securing Virtual Machines

The guest operating system that runs in the virtual machine is subject to the same security risks as a physical system. Secure virtual machines like physical machines, and follow best practices discussed in this document and in the *Security Configuration Guide* (formerly known as the *Hardening Guide*).

The *Security Configuration Guide* is available at https://core.vmware.com/security.

Activate or Deactivate UEFI Secure Boot for a Virtual Machine

UEFI Secure Boot is a security standard that helps ensure that your PC boots using only software that is trusted by the PC manufacturer. For certain virtual machine hardware versions and operating systems, you can activate secure boot just as you can for a physical machine.

You can activate secure boot only if all prerequisites are met. If prerequisites are not met, the check box is not visible in the vSphere Client.

- Verify that the virtual machine operating system and firmware support UEFI boot.
  - EFI firmware
  - Virtual hardware version 13 or later.
  - Operating system that supports UEFI secure boot.

  Note: Some guest operating systems do not support changing from BIOS boot to UEFI boot without guest OS modifications. Consult your guest OS documentation before changing to UEFI boot. If you upgrade a virtual machine that already uses UEFI boot to an operating system that supports UEFI secure boot, you can activate Secure Boot for that virtual machine.
- Turn off the virtual machine. If the virtual machine is running, the check box is dimmed.

In an operating system that supports UEFI secure boot, each piece of boot software is signed, including the bootloader, the operating system kernel, and operating system drivers. The virtual machine's default configuration includes several code signing certificates.

- A Microsoft certificate that is used only for booting Windows.
- A Microsoft certificate that is used for third-party code that is signed by Microsoft, such as Linux bootloaders.
- A VMware certificate that is used only for booting ESXi inside a virtual machine.

The virtual machine's default configuration includes one certificate for authenticating requests to modify the secure boot configuration, including the secure boot revocation list, from inside the virtual machine, which is a Microsoft KEK (Key Exchange Key) certificate.

In almost all cases, it is not necessary to replace the existing certificates. If you do want to replace the certificates, see the VMware Knowledge Base system.

VMware Tools version 10.1 or later is required for virtual machines that use UEFI secure boot. You can upgrade those virtual machines to a later version of VMware Tools when it becomes available.

For Linux virtual machines, VMware Host-Guest Filesystem is not supported in secure boot mode. Remove VMware Host-Guest Filesystem from VMware Tools before you activate secure boot.

Note: If you turn on secure boot for a virtual machine, you can load only signed drivers into that virtual machine.

This task describes how to use the vSphere Client to activate and deactivate secure boot for a virtual machine. You can also write scripts to manage virtual machine settings. For example, you can automate changing the firmware from BIOS to EFI for virtual machines with the following PowerCLI code:

```
$vm = Get-VM TestVM
```

```
$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

See *VMware PowerCLI User's Guide* for more information.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click the **VM Options** tab, and expand **Boot Options**.
4. Under **Boot Options**, ensure that firmware is set to **EFI**.
5. Select your task.
   - Select the **Secure Boot** check box to activate secure boot.
   - Deselect the **Secure Boot** check box to deactivate secure boot.
6. Click **OK**.

When the virtual machine boots, only components with valid signatures are allowed. The boot process stops with an error if it encounters a component with a missing or invalid signature.

Virtual Machine Security Best Practices

Following virtual machine security best practices helps ensure the integrity of your vSphere deployment.

General Virtual Machine Protection

A virtual machine is, in most respects, the equivalent of a physical server. Employ the same security measures in virtual machines that you do for physical systems.

Follow these best practices to protect your virtual machine:

Patches and other protection	Keep all security measures up-to-date, including applying appropriate patches. It is especially important to keep track of updates for dormant virtual machines that are powered off, because it can be easy to overlook them. For example, ensure that anti-virus software, anti-spy ware, intrusion detection, and other protection are enabled for every virtual machine in your virtual infrastructure. You should also ensure that you have enough space for the virtual machine logs.
Anti-virus scans	Because each virtual machine hosts a standard operating system, you must protect it from viruses by installing anti-virus software. Depending on how you are using the virtual machine, you might also want to install a software firewall. Stagger the schedule for virus scans, particularly in deployments with a large number of virtual machines. Performance of systems in your environment degrades significantly if you scan all virtual machines simultaneously. Because software firewalls and antivirus software can be virtualization-intensive, you can balance the need for these two security measures against virtual machine performance, especially if you are confident that your virtual machines are in a fully trusted environment.

Use Templates to Deploy Virtual Machines

When you manually install guest operating systems and applications on a virtual machine, you introduce a risk of misconfiguration. By using a template to capture a hardened base operating system image with no applications installed, you can ensure that all virtual machines are created with a known baseline level of security.

You can use templates that can contain a hardened, patched, and properly configured operating system to create other, application-specific templates, or you can use the application template to deploy virtual machines.

Provide templates for virtual machine creation that contain hardened, patched, and properly configured operating system deployments.

If possible, deploy applications in templates as well. Ensure that the applications do not depend on information specific to the virtual machine to be deployed.

Minimize Use of the Virtual Machine Console

The virtual machine console provides the same function for a virtual machine that a monitor provides on a physical server. Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls. Console access might therefore allow a malicious attack on a virtual machine.

1. Use native remote management services, such as terminal services and SSH, to interact with virtual machines.

   Grant access to the virtual machine console only when necessary.

2. Limit the connections to the virtual machine console.

   For example, in a highly secure environment, limit the connection to one. In some environments, you can increase the limit if several concurrent connections are necessary to accomplish normal tasks.

   a) In the vSphere Client, power off the virtual machine.
   b) Right-click the virtual machine and select **Edit Settings**.
   c) Click the **VM Options** tab, and expand **VMware Remote Console Options**.
   d) Enter the maximum number of sessions, for example, `2`.
   e) Click **OK**.

Prevent Virtual Machines from Taking Over Resources

When one virtual machine consumes so much of the host resources that other virtual machines on the host cannot perform their intended functions, a Denial of Service (DoS) might occur. To prevent a virtual machine from causing a DoS, use host resource management features such as setting Shares and using resource pools.

By default, all virtual machines on an ESXi host share resources equally. You can use Shares and resource pools to prevent a denial of service attack that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions.

Do not set limits or use resource pools until you fully understand the impact.

1. Provision each virtual machine with just enough resources (CPU and memory) to function properly.
2. Use Shares to guarantee resources to critical virtual machines.
3. Group virtual machines with similar requirements into resource pools.
4. In each resource pool, leave Shares set to the default to ensure that each virtual machine in the pool receives approximately the same resource priority.

   With this setting, a single virtual machine cannot use more than other virtual machines in the resource pool.

See the *vSphere Resource Management* documentation for information about shares and limits.

Disable Unnecessary Functions Inside Virtual Machines

Any service that is running in a virtual machine provides the potential for attack. By disabling system components that are not necessary to support the application or service that is running on the system, you reduce the potential.

Virtual machines do not usually require as many services or functions as physical servers. When you virtualize a system, evaluate whether a particular service or function is necessary.

Note: When possible, install guest operating systems using "minimal" or "core" installation modes to reduce the size, complexity, and attack surface of the guest operating system.

- Disable unused services in the operating system.

  For example, if the system runs a file server, turn off any Web services.
- Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adapters.
- Disable unused functionality, such as unused display features, or VMware Shared Folders, which enables sharing of host files to the virtual machine (Host Guest File System).
- Turn off screen savers.
- Do not run the X Window system on top of Linux, BSD, or Solaris guest operating systems unless it is necessary.

Remove Unnecessary Hardware Devices

Any enabled or connected device represents a potential attack channel. Users and processes with privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

An attacker with access to a virtual machine can connect a disconnected hardware device and access sensitive information on media that is left in a hardware device. The attacker can potentially disconnect a network adapter to isolate the virtual machine from its network, resulting in a denial of service.

- Do not connect unauthorized devices to the virtual machine.
- Remove unneeded or unused hardware devices.
- Disable unnecessary virtual devices from within a virtual machine.
- Ensure that only required devices are connected to a virtual machine. Virtual machines rarely use serial or parallel ports. As a rule, CD/DVD drives are connected only temporarily during software installation.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Disable hardware devices that are not required.

   Include checks for the following devices:

   - Serial ports
   - Parallel ports
   - USB controllers
   - CD-ROM drives

   Note: You must use PowerCLI commands to manage floppy drive devices in vSphere 7.0 and later.

Disable Unused Display Features

Attackers can use an unused display feature as a vector for inserting malicious code into your environment. Disable features that are not in use in your environment.

Power off the virtual machine.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. If appropriate, add or edit the following parameters.

Option	Description
svga.vgaonly	If you set this parameter to TRUE, advanced graphics functions no longer work. Do not set this parameter to TRUE with modern-day guest operating systems as they do not operate correctly. When `svga.vgaonly` is set to TRUE, only character-cell console mode is available. If you use this setting, `mks.enable3d` has no effect. **Note:** Apply this setting only to virtual machines that do not need a virtualized video card.
mks.enable3d	Set this parameter to FALSE on virtual machines that do not require 3D functionality.

Disable Unexposed Features

VMware virtual machines can work both in a vSphere environment and on hosted virtualization platforms such as VMware Workstation and VMware Fusion. Certain virtual machine parameters do not need to be enabled when you run a virtual machine in a vSphere environment. Disable these parameters to reduce the potential for vulnerabilities.

Turn off the virtual machine.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Set the following parameters to TRUE by adding or editing them.
   - `isolation.tools.memSchedFakeSampleStats.disable`
   - `isolation.tools.getCreds.disable`
   - `isolation.bios.bbs.disable`
   - `isolation.tools.hgfsServerSet.disable`

6. Click **OK**.

Disable VMware Shared Folders Sharing Host Files to the Virtual Machine

In high-security environments, you can disable certain components to minimize the risk that an attacker can use the host guest file system (HGFS) to transfer files inside the guest operating system.

Modifying the parameters described in this section affects only the Shared Folders feature and does not affect the HGFS server running as part of tools in the guest virtual machines. Also, these parameters do not affect the auto-upgrade and VIX commands that use the tools' file transfers.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Verify that the `isolation.tools.hgfsServerSet.disable` parameter is set to TRUE.

   A setting of TRUE prevents the VMX process from receiving a notification from each tool's service, daemon, or upgrader processes of its HGFS server capability.
6. Optional: Verify that the `isolation.tools.hgfs.disable` parameter is set to TRUE.

   A setting of TRUE disables the unused VMware Shared Folders feature for sharing host files to the virtual machine.

Disable Copy and Paste Operations Between Guest Operating System and Remote Console

Copy and paste operations between the guest operating system and remote console are disabled by default. For a secure environment, retain the default setting. If you require copy and paste operations, you must enable them using the vSphere Client.

Turn off the virtual machine.

The default values for these options are set to ensure a secure environment. However, you must set them to true explicitly if you want to enable audit tools to check that the setting is correct.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Ensure that the following values are in the Name and Value columns, or add them.

Name	Value
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true
isolation.tools.setGUIOptions.enable	false

   These options override any settings made in the guest operating system’s VMware Tools control panel.
6. Click **OK**.
7. Optional: If you made changes to the configuration parameters, restart the virtual machine.

Limiting Exposure of Sensitive Data Copied to the Clipboard

Copy and paste operations are disabled by default for hosts to prevent exposing sensitive data that has been copied to the clipboard.

When copy and paste is enabled on a virtual machine running VMware Tools, you can copy and paste between the guest operating system and remote console. When the console window gains focus, processes running in the virtual machine and non-privileged users can access the virtual machine console clipboard. If a user copies sensitive information to the clipboard before using the console, the use might expose sensitive data to the virtual machine. To prevent this problem, copy and paste operations for the guest operating system are disabled by default.

It is possible to enable copy and paste operations for virtual machines if necessary.

Restrict Users from Running Commands Within a Virtual Machine

By default, a user who has the vCenter Server Administrator role can interact with files and applications within a virtual machine's guest operating system. To reduce the risk of breaching guest confidentiality, availability, or integrity, create a nonguest access role without the **Guest Operations** privilege. Assign that role to administrators who do not need virtual machine file access.

Verify that you have **Administrator** privileges on the vCenter Server system where you create the role.

For security, be as restrictive about allowing access to the virtual data center as you are to the physical data center. Apply a custom role that disables guest access to users who require administrator privileges, but who are not authorized to interact with guest operating system files and applications.

For example, a configuration might include a virtual machine on the infrastructure that has sensitive information on it.

If tasks such as migration with vMotion require that data center administrators can access the virtual machine, disable some remote guest OS operations to ensure that those administrators cannot access sensitive information.

1. Log in to the vSphere Client as a user who has **Administrator** privileges on the vCenter Server system where you want to create the role.
2. Select **Administration** and click **Roles**.
3. Click the Administrator role and click the **Clone role action** icon.
4. Enter a role name and description and click **OK**.
   For example, type `Administrator No Guest Access`.
5. Select the cloned role and click the **Edit role action** icon.
6. Under the **Virtual machine** privilege, deselect **Guests operations** and click **Next**.
7. Click **Finish**.

Select the vCenter Server system or the host and assign a permission that pairs the user or group that should have the new privileges to the newly created role. Remove those users from the Administrator role.

Prevent a Virtual Machine User or Process from Disconnecting Devices

Users and processes without root or administrator privileges within virtual machines can connect or disconnect devices, such as network adapters and CD-ROM drives, and can modify device settings. To increase virtual machine security, remove these devices.

Turn off the virtual machine.

You can prevent virtual machine users in the guest OS, and processes running in the guest OS, from making any changes to the devices by changing the virtual machine advanced settings.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Verify that the following values are in the Name and Value columns, or add them.

Name	Value
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

   These settings do not affect a vSphere administrator's ability to connect or disconnect the devices attached to the virtual machine.

6. Click **OK** to close the Configuration Parameters dialog box, and click **OK** again.

Prevent Guest Operating System Processes from Sending Configuration Messages to the Host

To ensure that the guest operating system does not modify configuration settings, you can prevent these processes from writing any name-value pairs to the configuration file.

Turn off the virtual machine.

1. Browse to the virtual machine in the vSphere Client inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Click **Add Configuration Params** and enter the following values in the Name and Value columns.

Column	Value
Name	`isolation.tools.setinfo.disable`
Value	`true`

6. Click **OK** to close the Configuration Parameters dialog box, and click **OK** again.

Avoid Using Independent Nonpersistent Disks

When you use independent nonpersistent disks, successful attackers can remove any evidence that the machine was compromised by shutting down or rebooting the system. Without a persistent record of activity on a virtual machine, administrators might be unaware of an attack. Therefore, you should avoid using independent nonpersistent disks.

- Ensure that virtual machine activity is logged remotely on a separate server, such as a syslog server or equivalent Windows-based event collector.

  If remote logging of events and activity is not configured for the guest, scsiX:Y.mode should be one of the following settings:

  - Not present
  - Not set to independent nonpersistent

When nonpersistent mode is not enabled, you cannot roll a virtual machine back to a known state when you reboot the system.

Securing Virtual Machines with Intel Software Guard Extensions

vSphere enables you to configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines. Using vSGX enables you to provide additional security to your workloads.

Some modern Intel CPUs implement a security extension called Intel® Software Guard Extensions (Intel® SGX). Intel SGX is a processor-specific technology for application developers who seek to protect select code and data from disclosure or modification. Intel SGX allows user-level code to define private regions of memory, called enclaves. The enclave contents are protected such that code running outside the enclave cannot access the enclave contents.

vSGX enables virtual machines to use Intel SGX technology if available on the hardware. To use vSGX, the ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the BIOS of the ESXi host. You can use the vSphere Client to enable SGX for a virtual machine.

vSGX Overview

Virtual machines can use Intel SGX technology, if available on the hardware.

Requirements for vSGX

To use vSGX, your vSphere environment must meet these requirements:

- Virtual machine requirements:
  - EFI firmware
  - Hardware version 17 or later
- Component requirements:
  - vCenter Server 7.0 and later
  - ESXi 7.0 and later
- Guest OS support:
  - Linux
  - Windows Server 2016 (64 bit) and later
  - Windows 10 (64 bit) and later

Intel Hardware

For supported Intel hardware for vSGX, consult the VSphere Compatibility Guide at https://www.vmware.com/resources/compatibility/search.php.

You might need to turn off hyperthreading on certain CPUs to enable SGX on the ESXi host. For more information, see the VMware KB article at https://kb.vmware.com/s/article/71367.

Unsupported VMware Features on vSGX

The following features are not supported in a virtual machine when vSGX is enabled:

- vMotion/DRS migration
- Virtual machine suspend and resume
- Virtual machine snapshots (Virtual machine snapshots are supported if you do not snapshot the virtual machine's memory.)
- Fault tolerance
- Guest Integrity (GI, platform foundation for VMware AppDefense™ 1.0)

Note:

These VMware features are not supported due to how the Intel SGX architecture functions. They are not the result of a VMware shortcoming.

Enable vSGX on a Virtual Machine

You can enable vSGX on a virtual machine at the same time you create a virtual machine.

The ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the host's BIOS. See vSGX Overview for supported Intel CPUs.

Create a virtual machine that uses hardware version 17 or later and one of the following supported guest operating systems:

- Linux
- Windows 10 (64 bit) and later
- Windows Server 2016 (64 bit) and later

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object, select **New Virtual Machine**, and follow the prompts to create a virtual machine.

Option	Action
Select a creation type	Create a virtual machine.
Select a name and folder	Specify a name and target location.
Select a compute resource	Specify an object for which you have privileges to create virtual machines.
Select storage	In the VM storage policy, select the storage policy. Select a compatible datastore.
Select compatibility	Ensure that **ESXi 7.0 and later** is selected.
Select a guest OS	Select either Linux, Windows 10 (64-bit), or Windows Server 2016 (64-bit).
Customize hardware	Under Security devices, select the **Enable** check box for SGX. Under **VM Options** > **Boot Options** > **Firmware**, ensure that EFI is selected. Enter Enclave Page Cache (EPC) size and select Flexible Launch Control (FLC) mode accordingly.
Ready to complete	Review the information and click **Finish**.

Enable vSGX on an Existing Virtual Machine

You can enable vSGX on an existing virtual machine.

- The ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the host's BIOS. See vSGX Overview for supported Intel CPUs.
- The guest OS you use must be Linux, or Windows Server 2016 (64 bit) or later, or Windows 10 (64 bit) or later.
- The ESXi hosts running in your environment must be ESXi 7.0 or later.
- Verify that the virtual machine is turned off.
- The virtual machine must use EFI firmware.

- The virtual machine must use hardware version 17 or later.

You can enable vSGX for virtual machines running on vSphere 7.0 and later.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, under **Security devices**, select the **Enable** check box for SGX.
4. Enter Enclave Page Cache (EPC) size and select Flexible Launch Control (FLC) mode accordingly.
5. Under **VM Options** > **Boot Options** > **Firmware**, ensure that EFI is selected.
6. Click **OK**.

Remove vSGX from a Virtual Machine

You can remove vSGX from a virtual machine.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, under **Security devices**, deselect the **Enable** check box for SGX.
4. Click **OK**.
   Verify that the vSGX entry no longer appears in the virtual machine **Summary** tab in the **VM Hardware** pane.

Securing Virtual Machines with AMD Secure Encrypted Virtualization-Encrypted State

Secure Encrypted Virtualization-Encrypted State (SEV-ES) is a hardware feature enabled in recent AMD CPUs that keeps the guest operating system's memory and register state encrypted, protecting it against access from the hypervisor.

You can add SEV-ES to your virtual machines as an extra security enhancement. SEV-ES prevents CPU registers from leaking information in registers to components like the hypervisor. SEV-ES can also detect malicious modifications to a CPU register state.

vSphere and AMD Secure Encrypted Virtualization-Encrypted State

In vSphere 7.0 Update 1 and later, you can activate Secure Encrypted Virtualization-Encrypted State (SEV-ES) on supported AMD CPUs and guest operating systems.

Currently, SEV-ES supports only AMD EPYC 7xx2 CPUs (code named "Rome") and later CPUs, and only versions of Linux kernels that include specific support for SEV-ES.

SEV-ES Components and Architecture

The SEV-ES architecture consists of the following components.

- AMD CPU, specifically, the Platform Security Processor (PSP) that manages encryption keys and handles encryption.
- Enlightened operating system, that is, an operating system that uses guest-initiated calls to the hypervisor.
- Virtual Machine Monitor (VMM) and Virtual Machine Executable (VMX), to initialize an encrypted virtual machine state during virtual machine power-on, and also to handle calls from the guest operating system.
- VMkernel driver, to communicate unencrypted data between the hypervisor and the guest operating system.

Implementing and Managing SEV-ES on ESXi

You must first activate SEV-ES in a system's BIOS configuration. See the documentation for your system for more information about accessing the BIOS configuration. After you have activated SEV-ES in the BIOS for your system, you can then add SEV-ES to a virtual machine.

You use either the vSphere Client (starting in vSphere 7.0 Update 2) or PowerCLI commands to activate and deactivate SEV-ES on virtual machines. You can create new virtual machines with SEV-ES, or activate SEV-ES on existing virtual machines. Privileges to manage virtual machines activated with SEV-ES are the same as for managing regular virtual machines.

Unsupported VMware Features on SEV-ES

The following features are not supported when SEV-ES is activated.

- System Management Mode
- vMotion
- Powered-on snapshots (however, no-memory snapshots are supported)
- Hot add or remove of CPU or memory
- Suspend/resume
- VMware Fault Tolerance
- Clones and instant clones
- Guest Integrity
- UEFI Secure Boot

Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine with the vSphere Client

In vSphere 7.0 Update 2 and later, you can use the vSphere Client to add SEV-ES to a virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.
- SEV-ES must be enabled in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When enabling SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.

  Note: vSphere 7.0 Update 1 supports 16 SEV-ES enabled virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES enabled virtual machines per ESXi host.
- The ESXi host running in your environment must be at ESXi 7.0 Update 1 or later.
- The vCenter Server must be at vSphere 7.0 Update 2 or later.
- The guest operating system must support SEV-ES.

  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.

- The virtual machine must have the **Reserve all guest memory** option enabled, otherwise power-on fails.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object, select **New Virtual Machine**, and follow the prompts to create a virtual machine.

Option	Action
Select a creation type	Create a virtual machine.
Select a name and folder	Specify a name and target location.
Select a compute resource	Specify an object for which you have privileges to create virtual machines.
Select storage	In the VM storage policy, select the storage policy. Select a compatible datastore.
Select compatibility	Ensure that **ESXi 7.0 and later** is selected.
Select a guest OS	Select Linux, and select a version of Linux with specific support for SEV-ES.
Customize hardware	Under **VM Options** > **Boot Options** > **Firmware**, ensure that EFI is selected. Under **VM Options** > **Encryption**, select the **Enable** check box for AMD SEV-ES.
Ready to complete	Review the information and click **Finish**.

The virtual machine is created with SEV-ES.

Add AMD Secure Encrypted Virtualization-Encrypted State to a Virtual Machine

You can add SEV-ES to a virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.
- SEV-ES must be enabled in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When enabling SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.
  Note: vSphere 7.0 Update 1 supports 16 SEV-ES enabled virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES enabled virtual machines per ESXi host.
- The ESXi host running in your environment must be at ESXi 7.0 Update 1 or later.
- The guest operating system must support SEV-ES.
  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.
- The virtual machine must have the **Reserve all guest memory** option enabled, otherwise power-on fails.
- PowerCLI 12.1.0 or later must be installed on a system with access to your environment.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator to the vCenter Server that manages the ESXi host on which you want to add a virtual machine with SEV-ES.

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2. Create the virtual machine with the `New-VM` cmdlet, specifying `-SEVEnabled $true`.
   For example, first assign the host information to a variable, then create the virtual machine.
   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
   ```
   If you must specify the virtual hardware version, run the `New-VM` cmdlet with the `-HardwareVersion vmx-18` parameter. For example:
   ```
   New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true -HardwareVersion vmx-18
   ```

The virtual machine is created with SEV-ES.

Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine with the vSphere Client

In vSphere 7.0 Update 2 and later, you can use the vSphere Client to add SEV-ES to an existing virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.
- SEV-ES must be activated in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When activating SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.
  Note: vSphere 7.0 Update 1 supports 16 SEV-ES activated virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES activated virtual machines per ESXi host.
- The ESXi host running in your environment must be at ESXi 7.0 Update 1 or later.
- The vCenter Server must be at vSphere 7.0 Update 2 or later.
- The guest operating system must support SEV-ES.
  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.
- The virtual machine must have the **Reserve all guest memory** option checked, otherwise power-on fails.
- Ensure that the virtual machine is powered off.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. Under **VM Options** > **Boot Options** > **Firmware**, ensure that EFI is selected.
4. In the **Edit Settings** dialog box, under **VM Options** > **Encryption**, select the **Enable** check box for AMD SEV-ES.
5. Click **OK**.

SEV-ES is added to the virtual machine.

Activate AMD Secure Encrypted Virtualization-Encrypted State on an Existing Virtual Machine

You can add SEV-ES to an existing virtual machine to provide enhanced security to the guest operating system.

- The system must be installed with an AMD EPYC 7xx2 (code named "Rome") or later CPU and supporting BIOS.

- SEV-ES must be activated in the BIOS.
- The number of SEV-ES virtual machines per ESXi host is controlled by the BIOS. When activating SEV-ES in the BIOS, enter a value for the **Minimum SEV non-ES ASID** setting equal to the number of SEV-ES virtual machines plus one. For example, if you have 12 virtual machines that you want to run concurrently, enter `13`.
  Note: vSphere 7.0 Update 1 supports 16 SEV-ES activated virtual machines per ESXi host. Using a higher setting in the BIOS does not prevent SEV-ES from working, however, the limit of 16 still applies. vSphere 7.0 Update 2 supports 480 SEV-ES activated virtual machines per ESXi host.
- The ESXi host running in your environment must be ESXi 7.0 Update 1 or later.
- The guest operating system must support SEV-ES.
  Currently, only Linux kernels with specific support for SEV-ES are supported.
- The virtual machine must be at hardware version 18 or later.
- The virtual machine must have the **Reserve all guest memory** option checked, otherwise power-on fails.
- PowerCLI 12.1.0 or later must be installed on a system with access to your environment.
- Ensure that the virtual machine is powered off.

You can add SEV-ES to virtual machines running on ESXi 7.0 Update 1 or later.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator to the vCenter Server that manages the ESXi host with the virtual machine to which you want to add SEV-ES.
   For example:
   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```
2. Add SEV-ES to the virtual machine with the `Set-VM` cmdlet, specifying `-SEVEnabled $true`.
   For example:
   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
   ```
   If you must specify the virtual hardware version, run the `Set-VM` cmdlet with the `-HardwareVersion vmx-18` parameter. For example:
   ```
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
   ```

SEV-ES is added to the virtual machine.

Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine with the vSphere Client

In vSphere 7.0 Update 2 and later, you can use the vSphere Client to deactivate SEV-ES on a virtual machine.

- Ensure that the virtual machine is powered off.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, under **VM Options** > **Encryption**, deselect the **Enable** check box for AMD SEV-ES.
4. Click **OK**.

SEV-ES is deactivated on the virtual machine.

Deactivate AMD Secure Encrypted Virtualization-Encrypted State on a Virtual Machine

You can deactivate SEV-ES on a virtual machine.

- Ensure that the virtual machine is powered off.

- PowerCLI 12.1.0 or later must be installed on a system that has access to your environment.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator to the vCenter Server that manages the ESXi host with the virtual machine from which you want to remove SEV-ES.

   For example:

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. Deactivate SEV-ES on the virtual machine with the `Set-VM` cmdlet, specifying `-SEVEnabled $false`.

   For example, first assign the host information to a variable, then deactivate SEV-ES for the virtual machine.

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
   ```

SEV-ES is deactivated on the virtual machine.

Virtual Machine Encryption

With vSphere Virtual Machine Encryption, you can encrypt your sensitive workloads in an even more secure way. Access to encryption keys can be made conditional to the ESXi host being in a trusted state.

Before you can start with virtual machine encryption tasks, you must set up a key provider. The following key provider types are available.

Table 245: vSphere Key Providers

Key Provider	Description	For More Information
Standard key provider	Available in vSphere 6.5 and later, the standard key provider uses vCenter Server to request keys from an external key server. The key server generates and stores the keys, and passes them to vCenter Server for distribution.	See Configuring and Managing a Standard Key Provider.
Trusted key provider	Available in vSphere 7.0 and later, the vSphere Trust Authority trusted key provider makes access to the encryption keys conditional to the attestation state of a workload cluster. vSphere Trust Authority requires an external key server.	See vSphere Trust Authority.
VMware vSphere®Native Key Provider™	Available in vSphere 7.0 Update 2 and later, vSphere Native Key Provider is included in all vSphere editions and does not require an external key server.	See Configuring and Managing vSphere Native Key Provider.

Comparison of vSphere Key Providers

A high-level overview of the capabilities of the vSphere key providers requires your attention to help plan your encryption strategy.

In general, there is little difference in feature or product support between key provider daily operation. Though key providers look and behave similarly, you might have requirements and regulations to consider when choosing a key provider, as shown in the following table.

Table 246: Key Provider Considerations

Key Provider	External Key Server Required?	Quick Setup?	Works Only with vSphere?
Standard key provider	Yes	No	No
Trusted key provider	Yes	No	No
vSphere Native Key Provider	No	Yes	Yes

Encryption Features

The following encryption features are supported by each key provider type.

- Rekey using the same key provider or to another key provider
- Rotate keys
- Virtual Trusted Platform Module (vTPM)
- Disk encryption
- vSphere Virtual Machine Encryption
- Co-existence with other key providers
- Upgrade to a different key provider

vSphere Features

The following describes key provider support for some important vSphere features.

- Encrypted vSphere vMotion: Supported by all key provider types. The same key provider must be available on the destination host. See Encrypted vSphere vMotion.
- vCenter Server File-based Backup and Restore: Standard key provider and vSphere Native Key Provider support vCenter Server file-based backup and restore. Because most vSphere Trust Authority configuration information is stored on the ESXi hosts, the vCenter Server file-based backup mechanism does not back up this information. To ensure the configuration information for your vSphere Trust Authority deployment is saved, see Backing Up the vSphere Trust Authority Configuration.

VMware Products

The following table compares key provider support for some VMware products.

Table 247: Comparison of Support for VMware Products

Key Provider	vSAN	Site Recovery Manager	vSphere Replication
Standard key provider	Yes	Yes	Yes
Trusted key provider	Yes	Yes If the same vSphere Trust Authority services configuration is available on the recovery side, then SRM with array-based replication is supported.	No
vSphere Native Key Provider	Yes	Yes	Yes

Required Hardware

The following table compares some minimum key provider hardware requirements.

Table 248: Comparison of Required Hardware

Key Provider	TPM on ESXi Host
Standard key provider	Not required
Trusted key provider	Required on Trusted Hosts (hosts in the Trusted Cluster). **Note:** Currently, the ESXi hosts in the Trust Authority Cluster do not require a TPM. However, as a matter of best practice, consider installing new ESXi hosts with TPMs.
vSphere Native Key Provider	Not required vSphere Native Key Provider availability can optionally be restricted to hosts with a TPM.

Key Provider Naming

vSphere uses a key provider name to look up a key identifier. If two key providers have the same name, vSphere assumes that they are equivalent and have access to the same keys. Each logical key provider, regardless of its type (Standard, Trusted, and Native Key Provider), must have a unique name across all vCenter Server systems.

In a few instances, you configure the same key provider across multiple vCenter Server systems, such as:

- Migrating encrypted virtual machines between vCenter Server systems
- Setting up a vCenter Server as a disaster recovery site

How vSphere Virtual Machine Encryption Protects Your Environment

Regardless of which key provider you use, with vSphere Virtual Machine Encryption you can create encrypted virtual machines and encrypt existing virtual machines. Because all virtual machine files with sensitive information are encrypted, the virtual machine is protected. Only administrators with encryption privileges can perform encryption and decryption tasks.

Important: ESXi Shell users also have cryptographic operation privileges. For more information, see Prerequisites and Required Privileges for Encryption Tasks.

What Storage Does vSphere Virtual Machine Encryption Support

vSphere Virtual Machine Encryption works with any supported storage type (NFS, iSCSI, Fibre Channel, direct-attached storage, and so on), including VMware vSAN. For more information about using encryption on a vSAN cluster, see *Administering VMware vSAN* documentation.

vSphere Virtual Machine Encryption and vSAN use the same encryption libraries but they have different profiles. VM Encryption is a per-VM encryption and vSAN is a datastore level encryption.

vSphere Encryption Keys and Key Providers

vSphere uses two levels of encryption in the form of a Key Encryption Key (KEK) and a Data Encryption Key (DEK). Briefly, an ESXi host generates a DEK to encrypt virtual machines and disks. The KEK is provided by a key server, and encrypts (or "wraps") the DEK. The KEK encrypts the DEK using the AES256 algorithm and the DEK encrypts the VMDK using the XTS-AES-256 (512-bit key size) algorithm. Depending on the type of key provider, different methods are used to create and manage the DEK and KEK.

Standard key provider operates as follows.

1. The ESXi host generates and uses internal keys to encrypt virtual machines and disks. These keys are used as DEKs.

2. vCenter Server requests keys from the key server (KMS). These keys are used as the KEKs. vCenter Server stores only the ID of each KEK, but not the key itself.
3. ESXi uses the KEK to encrypt the internal keys, and stores the encrypted internal key on disk. ESXi does not store the KEK on disk. If a host reboots, vCenter Server requests the KEK with the corresponding ID from the key server and makes it available to ESXi. ESXi can then decrypt the internal keys as needed.

vSphere Trust Authority trusted key provider operates as follows.

1. The vCenter Server of the Trusted Cluster checks if the default trusted key provider is accessible to the ESXi host where the encrypted virtual machine is to be created.
2. The vCenter Server of the Trusted Cluster adds the trusted key provider to the virtual machine ConfigSpec.
3. The virtual machine creation request is sent to the ESXi host.
4. If an attestation token is not already available to the ESXi host, it requests one from the Attestation Service.
5. The Key Provider Service validates the attestation token and creates a KEK to be sent to the ESXi host. The KEK is wrapped (encrypted) with the primary key that is configured on the key provider. Both the KEK ciphertext and KEK plaintext are returned to the Trusted Host.
6. The ESXi host generates a DEK to encrypt the virtual machine disks.
7. The KEK is used to wrap the DEK generated by the ESXi host, and the ciphertext from the key provider is stored alongside the encrypted data.
8. The virtual machine is encrypted and written to storage.

Note: If you delete or unregister an encrypted virtual machine, the ESXi host and the cluster remove the KEK from cache. The ESXi host can no longer use the KEK. This behavior is the same for standard key providers and trusted key providers.

vSphere Native Key Provider operates as follows.

1. When you create the key provider, vCenter Server generates a primary key and pushes it to the ESXi hosts in the cluster. (No external key server is involved.)
2. The ESXi hosts generate a DEK on demand.
3. When you perform an encryption activity, data is encrypted with the DEK.
   Encrypted DEKs are stored alongside the encrypted data.
4. When you decrypt data, the primary key is used to decrypt the DEK, and then the data.

What Is Encrypted

vSphere Virtual Machine Encryption supports encryption of virtual machine files, virtual disk files, and core dump files.

Virtual machine files

Most virtual machine files, in particular, guest data that are not stored in the VMDK file, are encrypted. This set of files includes but is not limited to the NVRAM, VSWP, and VMSN files. The key from the key provider unlocks an encrypted bundle in the VMX file that contains internal keys and other secrets. The key retrieval works as follows, depending on the key provider:

- Standard key provider: vCenter Server manages the keys from the key server and ESXi hosts cannot directly access the key provider. The hosts wait for vCenter Server to push the keys.
- Trusted key provider and vSphere Native Key Provider: The ESXi hosts directly access the key providers, and so fetch the requested keys either from the vSphere Trust Authority service directly or the vSphere Native Key Provider.

When you use the vSphere Client to create an encrypted virtual machine, you can encrypt and decrypt virtual disks separate from virtual machine files. All virtual disks are encrypted by default.

	For other encryption tasks, such as encrypting an existing virtual machine, you can encrypt and decrypt virtual disks separate from virtual machine files. **Note:** You cannot associate an encrypted virtual disk with a virtual machine that is not encrypted.
Virtual disk files	Data in an encrypted virtual disk (VMDK) file is never written in cleartext to storage or physical disk, and is never transmitted over the network in cleartext. The VMDK descriptor file is mostly cleartext, but contains a key ID for the KEK and the internal key (DEK) in the encrypted bundle. You can use the vSphere API to perform either a shallow recrypt operation with a new KEK or deep recrypt operation with a new internal key.
Core dumps	Core dumps on an ESXi host that has encryption mode enabled are always encrypted. See vSphere Virtual Machine Encryption and Core Dumps. Core dumps on the vCenter Server system are not encrypted. Protect access to the vCenter Server system.

Note: For information on some limitations concerning devices and features that vSphere Virtual Machine Encryption can interoperate with, see Virtual Machine Encryption Interoperability.

What Is Not Encrypted

Some of the files that are associated with a virtual machine are not encrypted or partially encrypted.

Log files	Log files are not encrypted because they do not contain sensitive data.
Virtual machine configuration files	Most of the virtual machine configuration information, stored in the VMX and VMSD files, is not encrypted.
Virtual disk descriptor file	To support disk management without a key, most of the virtual disk descriptor file is not encrypted.

Who Can Perform Cryptographic Operations

Only users that are assigned the **Cryptographic Operations** privileges can perform cryptographic operations. The privilege set is fine grained. The default Administrator system role includes all **Cryptographic Operations** privileges. The No Cryptography Administrator role supports all Administrator privileges except for the **Cryptographic Operations** privileges.

In addition to using the **Cryptographer.*** privileges, vSphere Native Key Provider can use the **Cryptographer.ReadKeyServersInfo** privilege, which is specific to vSphere Native Key Providers.

See Cryptographic Operations Privileges for more information.

You can create additional custom roles, for example, to allow a group of users to encrypt virtual machines but to prevent them from decrypting virtual machines.

How Can I Perform Cryptographic Operations

The vSphere Client supports many of the cryptographic operations. For other tasks, you can use the vSphere API.

Table 249: Interfaces for Performing Cryptographic Operations

Interface	Operations	Information
vSphere Client	Create encrypted virtual machine Encrypt and decrypt virtual machines	This book
PowerCLI	Create encrypted virtual machine Encrypt and decrypt virtual machines Configure vSphere Trust Authority	*VMware PowerCLI Cmdlets Reference*
vSphere Web Services SDK	Create encrypted virtual machine Encrypt and decrypt virtual machines Perform a deep recrypt of a virtual machine (use a different DEK) Perform a shallow recrypt of a virtual machine (use a different KEK)	*vSphere Web Services SDK Programming Guide* *vSphere Web Services API Reference*
`crypto-util`	Decrypt encrypted core dumps Check whether files are encrypted Perform other management tasks directly on the ESXi host	Command-line help vSphere Virtual Machine Encryption and Core Dumps

Recrypting Virtual Machines

You can recrypt a virtual machine with new keys, for example, in case a key expires or becomes compromised. The following options are available.

- A deep recrypt, which replaces both the Disk Encryption Key (DEK) and Key Encryption Key (KEK)
- A shallow recrypt, which replaces only the KEK

You must perform a recrypt of a virtual machine by using the API. See *vSphere Web Services SDK Programming Guide*.

A deep recrypt requires that the virtual machine is powered off and contains no snapshots. You can perform a shallow recrypt operation while the virtual machine is powered on, and if the virtual machine has snapshots present. Shallow recrypt of an encrypted virtual machine with snapshots is permitted only on a single snapshot branch (disk chain). Multiple snapshot branches are not supported. Also, shallow recrypt is not supported on a linked clone of a virtual machine or disk. If the shallow recrypt fails before updating all links in the chain with the new KEK, you can still access the encrypted virtual machine if you have the old and new KEKs. However, it is best to reissue the shallow recrypt operation before performing any snapshot operations.

vSphere Virtual Machine Encryption Components

Depending on which key provider you use, an external key server, the vCenter Server system, and your ESXi hosts are potentially contributing to the encryption solution.

The following components comprise vSphere Virtual Machine Encryption:

- An external key server, also called a KMS (not required for vSphere Native Key Provider)
- vCenter Server
- ESXi hosts

Key Server

The key server is a Key Management Interoperability Protocol (KMIP) management server that is associated with a key provider. A standard key provider and a trusted key provider require a key server. vSphere Native Key Provider does not require a key server. The following table describes the differences in key provider and key server interaction.

Table 250: Key Providers and Key Server Interaction

Key Provider	Interaction with Key Server
Standard key provider	A standard key provider uses vCenter Server to request keys from a key server. The key server generates and stores the keys, and passes them to vCenter Server for distribution to the ESXi hosts.
Trusted key provider	A trusted key provider uses a Key Provider Service that enables the trusted ESXi hosts to fetch the keys directly. See What Is the vSphere Trust Authority Key Provider Service.
vSphere Native Key Provider	vSphere Native Key Provider does not require a key server. vCenter Server generates a primary key and pushes it to the ESXi hosts. The ESXi hosts then generate data encryption keys (even when not connected to vCenter Server). See vSphere Native Key Provider Overview.

You can use the vSphere Client or the vSphere API to add key provider instances to the vCenter Server system. If you use multiple key provider instances, all instances must be from the same vendor and must replicate keys.

If your environment uses different key server vendors in different environments, you can add a key provider for each key server and specify a default key provider. The first key provider that you add becomes the default key provider. You can explicitly specify the default later.

As a KMIP client, vCenter Server uses the Key Management Interoperability Protocol (KMIP) to make it easy to use the key server of your choice.

vCenter Server

The following table describes the role of vCenter Server in the encryption process.

Table 251: Key Providers and vCenter Server

Key Provider	Role of vCenter Server	How Are Privileges Checked
Standard key provider	Only vCenter Server has the credentials for logging in to the key server. Your ESXi hosts do not have those credentials. vCenter Server obtains keys from the key server and pushes them to the ESXi hosts. vCenter Server does not store the key server keys, but keeps a list of key IDs.	vCenter Server checks the privileges of users who perform cryptographic operations.
Trusted key provider	vSphere Trust Authority removes the need for vCenter Server to request keys from the key server, and makes access to the encryption keys conditional to the attestation state of a workload cluster. You must use separate vCenter Server systems for the Trusted Cluster and Trust Authority Cluster.	vCenter Server checks the privileges of users who perform cryptographic operations. Only users who are members of the TrustedAdmins SSO group can perform administrative operations.
vSphere Native Key Provider	The vCenter Server generates the keys.	vCenter Server checks the privileges of users who perform cryptographic operations.

You can use the vSphere Client to assign cryptographic operation privileges or to assign the **No cryptography administrator** custom role to groups of users. See Prerequisites and Required Privileges for Encryption Tasks.

vCenter Server adds cryptography events to the list of events that you can view and export from the vSphere Client Event Console. Each event includes the user, time, key ID, and cryptographic operation.

The keys that come from the key server are used as key encryption keys (KEKs).

ESXi Hosts

ESXi hosts are responsible for several aspects of the encryption workflow.

Table 252: ESXi Hosts

Key Provider	ESXi Host Aspects
Standard key provider	• vCenter Server pushes keys to an ESXi host when the host needs a key. The host must have encryption mode enabled. The current user's role must include cryptographic operation privileges. See Prerequisites and Required Privileges for Encryption Tasks and Cryptographic Operations Privileges. • Ensuring that guest data for encrypted virtual machines is encrypted when stored on disk. • Ensuring that guest data for encrypted virtual machines is not sent over the network without encryption.
Trusted key provider	The ESXi hosts run vSphere Trust Authority services, depending on if they are Trusted Hosts or Trust Authority Hosts. Trusted ESXi hosts run workload virtual machines that can be encrypted using key providers published by the Trust Authority Hosts. See Trusted Infrastructure Overview.
vSphere Native Key Provider	The ESXi hosts fetch keys directly from the vSphere Native Key Provider.

The keys that the ESXi host generates are called internal keys in this document. These keys typically act as data encryption keys (DEKs).

Encryption Process Flow

After you set up a key provider, users with the required privileges can create encrypted virtual machines and disks. Those users can also encrypt existing virtual machines and decrypt encrypted virtual machines, and add Virtual Trusted Platform Modules (vTPMs) to virtual machines.

Depending on the key provider type, the process flow can involve a key server, the vCenter Server, and the ESXi host.

Standard Key Provider Encryption Process Flow

During the encryption process, different vSphere components interact as follows.

1. When the user performs an encryption task, for example, creating an encrypted virtual machine, vCenter Server requests a new key from the default key server. This key is used as the KEK.
2. vCenter Server stores the key ID and passes the key to the ESXi host. If the ESXi host is part of a cluster, vCenter Server sends the KEK to each host in the cluster.
   The key itself is not stored on the vCenter Server system. Only the key ID is known.

3. The ESXi host generates internal keys (DEKs) for the virtual machine and its disks. It keeps the internal keys in memory only, and uses the KEKs to encrypt internal keys.
   Unencrypted internal keys are never stored on disk. Only encrypted data is stored. Because the KEKs come from the key server, the host continues to use the same KEKs.
4. The ESXi host encrypts the virtual machine with the encrypted internal key.
   Any hosts that have the KEK and that can access the encrypted key file can perform operations on the encrypted virtual machine or disk.

Trusted Key Provider Encryption Process Flow

The vSphere Trust Authority encryption process flow includes the vSphere Trust Authority services, the trusted key providers, the vCenter Server, and the ESXi hosts.

Encrypting a virtual machine with a trusted key provider looks the same as the virtual machine encryption user experience when using a standard key provider. Virtual machine encryption under vSphere Trust Authority continues to rely on either virtual machine encryption storage policies, or the presence of a vTPM device, to decide when to encrypt a virtual machine. You still use a default configured key provider (called a KMS cluster in vSphere 6.5 and 6.7) when encrypting a virtual machine from the vSphere Client. And, you can still use the APIs in a similar way to specify the key provider manually. The existing Cryptographic privileges added for vSphere 6.5 are still relevant in vSphere 7.0 for vSphere Trust Authority.

The encryption process for the trusted key provider has some important differences from the standard key provider:

- Trust Authority administrators do not specify information directly when setting up a key server for a vCenter Server instance, and they do not establish the key server trust. Instead, vSphere Trust Authority publishes trusted key providers that the Trusted Hosts can use.
- vCenter Server no longer pushes keys to ESXi hosts and instead it can treat each trusted key provider as a single top-level key.
- Only Trusted Hosts can request encryption operations from Trust Authority Hosts.

vSphere Native Key Provider Encryption Process Flow

vSphere Native Key Provider is included in vSphere starting with the 7.0 Update 2 release. When you configure a vSphere Native Key Provider, vCenter Server pushes a primary key to all ESXi hosts in the cluster. Likewise, if you update or delete a vSphere Native Key Provider, the change is pushed to the hosts in the cluster. The encryption process flow is similar to how a trusted key provider works. The difference is that vSphere Native Key Provider generates the keys and wraps them with the primary key, then hands them back to perform encryption.

Custom Attributes for Key Servers

The Key Management Interoperability Protocol (KMIP) supports adding custom attributes intended for vendor-specific purposes. Custom attributes enable you to more specifically identify keys stored in your key server. vCenter Server adds the following custom attributes for virtual machine keys and host keys.

Table 253: Virtual Machine Encryption Custom Attributes

Custom Attribute	Value
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server version
`x-Component`	Virtual Machine
`x-Name`	Virtual machine name (gathered from ConfigInfo or ConfigSpec)

Custom Attribute	Value
x-Identifier	Virtual machine's instanceUuid (gathered from ConfigInfo or ConfigSpec)

Table 254: Host Encryption Custom Attributes

Custom Attribute	Value
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server version
x-Component	ESXi Server
x-Name	Host name
x-Identifier	Host's hardware Uuid

vCenter Server adds the `x-Vendor` , `x-Product` , and `x-Product_Version` attributes when the key server creates a key. When the key is used to encrypt a virtual machine or host, vCenter Server sets the `x-Component` , `x-Identifier` , and `x-Name` attributes. You might be able to view these custom attributes in your key server user interface. Check with your key server vendor.

Both the host key and virtual machine key have the six custom attributes. `x-Vendor` , `x-Product` , and `x-Product_Version` might be the same for both keys. These attributes are set when the key is generated. Depending on if the key is for a virtual machine or a host, it might have `x-Component` , `x-Identifier` , and `x-Name` attributes appended.

Key Errors

When an error occurs sending keys from the key server to an ESXi host, vCenter Server generates a message in the event log for the following events:

- Adding keys to the ESXi host failed due to host connection or host support issues.
- Getting keys from the key server failed due to key missing in the key server.
- Getting keys from the key server failed due to the key server connection.

Decrypting Encrypted Virtual Machines

If you later want to decrypt an encrypted virtual machine, you change its storage policy. You can change the storage policy for the virtual machine and all disks. If you want to decrypt individual components, decrypt selected disks first, then decrypt the virtual machine by changing the storage policy for VM Home. Both keys are required for decryption of each component. See Decrypt an Encrypted Virtual Machine or Virtual Disk.

Virtual Disk Encryption

When you create an encrypted virtual machine from the vSphere Client, you can decide which disks to exclude from encryption. You can later add disks and set their encryption policies. You cannot add an encrypted disk to a virtual machine that is not encrypted, and you cannot encrypt a disk if the virtual machine is not encrypted.

Encryption for a virtual machine and its disks is controlled through storage policies. The storage policy for VM Home governs the virtual machine itself, and each virtual disk has an associated storage policy.

- Setting the storage policy of VM Home to an encryption policy encrypts only the virtual machine itself.
- Setting the storage policy of VM Home and all the disks to an encryption policy encrypts all components.

Consider the following use cases.

Table 255: Virtual Disk Encryption Use Cases

Use Case	Details
Create an encrypted virtual machine.	If you add disks while creating an encrypted virtual machine, the disks are encrypted by default. You can change the policy not to encrypt one or more of the disks. After virtual machine creation, you can explicitly change the storage policy for each disk. See Change the Encryption Policy for Virtual Disks.
Encrypt a virtual machine.	To encrypt an existing virtual machine, you change its storage policy. You can change the storage policy for the virtual machine and all virtual disks. To encrypt just the virtual machine, you can specify an encryption policy for VM Home and select a different storage policy, such as Datastore Default, for each virtual disk. See Create an Encrypted Virtual Machine.
Add an existing unencrypted disk to an encrypted virtual machine (encryption storage policy).	Fails with an error. You have to add the disk with the default storage policy, but can later change the storage policy. See Change the Encryption Policy for Virtual Disks.
Add an existing unencrypted disk to an encrypted virtual machine with a storage policy that does not include encryption, for example Datastore Default.	The disk uses the default storage policy. You can explicitly change the storage policy after adding the disk if you want an encrypted disk. See Change the Encryption Policy for Virtual Disks.
Add an encrypted disk to an encrypted virtual machine. VM Home storage policy is Encryption.	When you add the disk, it remains encrypted. The vSphere Client displays the size and other attributes, including encryption status.
Add an existing encrypted disk to an unencrypted virtual machine.	Prior to vSphere 7.0 Update 3i, you cannot encrypt the virtual disk of an unencrypted virtual machine. In vSphere Update 3i and later, the vSphere Client prompts if you want to reconfigure the unencrypted virtual machine with the encrypted disk by encrypting VM Home.
Register an encrypted virtual machine.	If you remove an encrypted virtual machine from vCenter Server but do not delete it from disk, you can return it to the vCenter Server inventory by registering the VM's virtual machine configuration (.vmx) file. To register the encrypted VM, the user must have the **Cryptographic operations** > **Register VM** privilege. If the VM was encrypted using a standard key provider, when the encrypted VM is registered, vCenter Server pushes the required keys to the ESXi host. If the user registering the VM does not have the **Cryptographic operations** > **Register VM** privilege, vCenter Server locks the VM upon registration, and the VM is not usable until it is unlocked. If the VM was encrypted using a trusted key provider or vSphere Native Key Provider, when the encrypted VM is registered, vCenter Server no longer pushes keys to the ESXi host. Instead, the keys are fetched from the host when the VM is registered. If the user registering the VM does not have the **Cryptographic operations** > **Register VM** privilege, vCenter Server does not permit the operation.

Virtual Machine Encryption Errors

If vCenter Server detects a critical error with virtual machine encryption, it creates an event. You can view these events to help troubleshoot and resolve encryption errors.

vCenter Server creates events for the following virtual machine encryption critical errors.

- Failure to generate a KEK.
- Insufficient disk space on the datastore to create an encrypted virtual machine.
- Insufficient user privilege to initiate encryption operation.
- The specified key is missing on the key provider and so the ESXi host key is renewed with a new key.
- An error occurred on the key provider with the specified key and so the ESXi host key is renewed with a new key.

Prerequisites and Required Privileges for Encryption Tasks

Encryption tasks are possibly only in environments that includevCenter Server. In addition, theESXi host must have encryption mode enabled for most encryption tasks. The user who performs the task must have the appropriate privileges. A set of**Cryptographic Operations** privileges allows fine-grained control. If virtual machine encryption tasks require a change to the host encryption mode, additional privileges are required.

Note: vSphere Trust Authority has additional prerequisites and required privileges. See Prerequisites and Required Privileges for vSphere Trust Authority.

Cryptography Privileges and Roles

By default, the user with thevCenter Server Administrator role has all privileges. The**No cryptography administrator** role does not have the following privileges that are required for cryptographic operations.

Important: ESXi Shell users also have cryptographic operation privileges.

- Add**Cryptographic Operations** privileges.
- **Global** > **Diagnostics**
- **Host** > **Inventory** > **Add host to cluster**
- **Host** > **Inventory** > **Add standalone host**
- **Host** > **Local operations** > **Manage user groups**

You can assign the**No cryptography administrator** role tovCenter Server administrators that do not need**Cryptographic Operations** privileges.

To impose more limits on what users can do, you can clone the**No cryptography administrator** role and create a custom role with only some of the**Cryptographic Operations** privileges. For example, you can create a role that allows users to encrypt but not to decrypt virtual machines. See Using Roles to Assign Privileges.

Host Encryption Mode

Host encryption mode determines if anESXi host is ready to accept cryptographic material for encrypting virtual machines and virtual disks. Before any cryptographic operations can occur on a host, host encryption mode must be enabled. Host encryption mode is often enabled automatically when it is required, but you can enable it explicitly. You can check and explicitly set the current host encryption mode from thevSphere Client or by using the vSphere API.

When host encryption mode is enabled,vCenter Server installs a host key on the host, which ensures that the host is cryptographically "safe." With the host key in place, other cryptographic operations can proceed, includingvCenter Server obtaining keys from the key provider and pushing them to the ESXi hosts.

In "safe" mode, user worlds (that is, hostd) and encrypted virtual machines have their core dumps encrypted. Unencrypted virtual machines do not have their core dumps encrypted.

For more information about encrypted core dumps and how they are used by VMware Technical Support, see the VMware knowledge base article at http://kb.vmware.com/kb/2147388.

For instructions, see Enable Host Encryption Mode Explicitly.

After Host encryption mode is enabled, it cannot be disabled easily. See Disable Host Encryption Mode Using the API.

Automatic changes occur when encryption operations attempt to enable host encryption mode. For example, assume that you add an encrypted virtual machine to a standalone host. Host encryption mode is not enabled. If you have the required privileges on the host, encryption mode changes to enabled automatically.

Assume that a cluster has threeESXi hosts, host A, B, and C. You create an encrypted virtual machine on host A. What happens depends on several factors.

- If hosts A, B, and C already have encryption enabled, you need only**Cryptographic operations** > **Encrypt new** privileges to create the virtual machine.
- If hosts A and B are enabled for encryption and C is not enabled, the system proceeds as follows.
  - Assume that you have both the**Cryptographic operations** > **Encrypt new** and the**Cryptographic operations** > **Register host** privileges on each host. In that case, the virtual machine creation process enables encryption on host C. The encryption process enables host encryption mode on host C, and pushes the key to each host in the cluster.

    For this case, you can also explicitly enable host encryption on host C.
  - Assume that you have only**Cryptographic operations** > **Encrypt new** privileges on the virtual machine or virtual machine folder. In that case, virtual machine creation succeeds and the key becomes available on host A and host B. Host C remains disabled for encryption and does not have the virtual machine key.
- If none of the hosts has encryption enabled, and you have**Cryptographic operations** > **Register host** privileges on host A, then the virtual machine creation process enables host encryption on that host. Otherwise, an error results.
- You can also use the vSphere API to set the encryption mode of a cluster to "force enable." Force enable causes all hosts in the cluster to be cryptographically "safe," that is,vCenter Server has installed a host key on the host. See *vSphere Web Services SDK Programming Guide*.

Disk Space Requirements

When you encrypt an existing virtual machine, you need at least twice the space that the virtual machine is currently using.

Encrypted vSphere vMotion

vSphere vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options.

Encrypted vSphere vMotion secures confidentiality, integrity, and authenticity of data that is transferred with vSphere vMotion. vSphere supports encrypted vMotion of unencrypted and encrypted virtual machines across vCenter Server instances.

What Is Encrypted

For encrypted disks, the data is transmitted encrypted in all cases. For unencrypted disks, the following applies:

- If disk data is transferred within a host, that is without changing the host, you change only the datastore, the transfer is unencrypted.
- If disk data is transferred between hosts and encrypted vMotion is used, the transfer is encrypted. If encrypted vMotion is not used the transfer is unencrypted.

For virtual machines that are encrypted, migration with vSphere vMotion always uses encrypted vSphere vMotion. You cannot turn off encrypted vSphere vMotion for encrypted virtual machines.

Encrypted vSphere vMotion States

For virtual machines that are not encrypted, you can set encrypted vSphere vMotion to one of the following states. The default is Opportunistic.

Disabled	Do not use encrypted vSphere vMotion.
Opportunistic	Use encrypted vSphere vMotion if source and destination hosts support it. Only ESXi versions 6.5 and later use encrypted vSphere vMotion.
Required	Allow only encrypted vSphere vMotion. If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.

When you encrypt a virtual machine, the virtual machine keeps a record of the current encrypted vSphere vMotion setting. If you later activated encryption for the virtual machine, the encrypted vMotion setting remains at Required until you change the setting explicitly. You can change the settings using **Edit Settings**.

Note:

Currently, you must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances. See *vSphere Web Services SDK Programming Guide* and *vSphere Web Services API Reference*.

Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances

vSphere vMotion supports migrating and cloning encrypted virtual machines across vCenter Server instances.

When migrating or cloning encrypted virtual machines across vCenter Server instances, the source and destination vCenter Server instances must be configured to share the key provider that was used to encrypt the virtual machine. In addition, the key provider name must be the same on both the source and destination vCenter Server instances and have the following characteristics:

- Standard key provider: The same key server (or key servers) must be in the key provider.
- Trusted key provider: The same vSphere Trust Authority service must be configured on the destination host.
- vSphere Native Key Provider: Must have the same KDK.

The destination vCenter Server ensures the destination ESXi host has encryption mode enabled, ensuring the host is cryptographically "safe."

The following privileges are required when using vSphere vMotion to migrate or clone an encrypted virtual machine across vCenter Server instances.

- Migrating: **Cryptographic operations** > **Migrate** on the virtual machine
- Cloning: **Cryptographic operations** > **Clone** on the virtual machine

Also, the destination vCenter Server must have the **Cryptographic operations** > **EncryptNew** privilege. If the destination ESXi host is not in "safe" mode, the **Cryptographic operations** > **RegisterHost** privilege must also be on the destination vCenter Server.

Certain tasks are not allowed when migrating virtual machines (non-encrypted or encrypted), either on the same vCenter Server or across vCenter Server instances.

- You cannot change the VM Storage Policy.
- You cannot perform a key change.

Note:

You can change the VM Storage Policy while cloning virtual machines.

Minimum Requirements for Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances

The minimum version requirements for migrating or cloning standard key provider encrypted virtual machines across vCenter Server instances using vSphere vMotion are:

- Both the source and destination vCenter Server instances must be on version 7.0 or later.
- Both the source and destination ESXi hosts must be on version 6.7 or later.

The minimum version requirements for migrating or cloning trusted key provider encrypted virtual machines across vCenter Server instances using vSphere vMotion are:

- The vSphere Trust Authority service must be configured for the destination host and the destination host must be attested.
- Encryption cannot change on migration. For example, an unencrypted disk cannot be encrypted while the virtual machine is migrated to the new storage.
- You can migrate a standard encrypted virtual machine onto a Trusted Host. The key provider name must be the same on both the source and destination vCenter Server instances.
- You cannot migrate a vSphere Trust Authority encrypted virtual machine onto a non-Trusted Host.

Trusted Key Provider vMotion and Cross-vCenter Server vMotion

Trusted key provider fully supports vMotion across ESXi hosts.

Cross-vCenter Server vMotion is supported, but with the following restrictions.

1. The required trusted service must be configured on the destination host and the destination host must be attested.
2. Encryption cannot change on migration. For example, a disk cannot be encrypted while the virtual machine is migrated to the new storage.

When performing cross-vCenter Server vMotion, vCenter Server checks that the trusted key provider is available on the destination host, and if the host has access to it.

vSphere Native Key Provider vMotion and Cross-vCenter Server vMotion

vSphere Native Key Provider supports vMotion and Encrypted vMotion across ESXi hosts. Cross-vCenter Server vMotion is supported if vSphere Native Key Provider is configured on the destination host.

Encryption Best Practices, Caveats, and Interoperability

Any best practices and caveats that apply to the encryption of physical machines apply to virtual machine encryption as well. The virtual machine encryption architecture results in some additional recommendations. As you are planning your virtual machine encryption strategy, consider interoperability limitations.

Note:

For information about vSphere Trust Authority interoperability, see vSphere Trust Authority Best Practices, Caveats, and Interoperability.

Virtual Machine Encryption Best Practices

Follow virtual machine encryption best practices to avoid problems later, for example, when you generate a `vm-support` bundle.

General Best Practices

To avoid problems, follow these general best practices.

- Do not encrypt any vCenter Server appliance virtual machines.

- If your ESXi host fails, retrieve the support bundle as soon as possible. The host key must be available for generating a support bundle that uses a password, or for decrypting a core dump. If the host is rebooted, it is possible that the host key changes. If that happens, you can no longer generate a support bundle with a password or decrypt core dumps in the support bundle with the host key.
- Manage key provider names carefully. If the key provider name changes for a key server that is already in use, a VM that is encrypted with keys from that key server enters a locked state during power-on or register. In that case, remove the key server from the vCenter Server and add it with the key provider name that you used initially.
- Do not edit VMX files and VMDK descriptor files. These files contain the encryption bundle. It is possible that your changes make the virtual machine unrecoverable, and that the recovery problem cannot be fixed.
- The vSphere Virtual Machine Encryption process encrypts data on the host before writing the data to storage. The effectiveness of back-end storage features such as deduplication, compression, replication, and so on, might be affected when encrypting virtual machines in this manner.
- If you use multiple layers of encryption, for example, vSphere Virtual Machine Encryption and in-guest encryption (BitLocker, dm-crypt, and so on), overall virtual machine performance might be affected, because the encryption processes use additional CPU and memory resources.
- Ensure that replicated copies of virtual machines encrypted with vSphere Virtual Machine Encryption have access to the encryption keys at the recovery site. For standard key providers, this is handled as part of the design of the Key Management System, outside of vSphere. For vSphere Native Key Provider, ensure that a backup copy of the Native Key Provider key exists and is protected against loss. For more information, see Back up a vSphere Native Key Provider.
- Encryption is CPU intensive. AES-NI significantly improves encryption performance. Enable AES-NI in your BIOS.

Best Practices for Encrypted Core Dumps

Follow these best practices to avoid having problems when you want to examine a core dump to diagnose a problem.

- Establish a policy regarding core dumps. Core dumps are encrypted because they can contain sensitive information such as keys. If you decrypt a core dump, consider it sensitive information. ESXi core dumps might contain keys for the ESXi host and for the virtual machines on it. Consider changing the host key and recrypting encrypted virtual machines after you decrypt a core dump. You can perform both tasks by using the vSphere API.
  See vSphere Virtual Machine Encryption and Core Dumps for details.
- Always use a password when you collect a `vm-support` bundle. You can specify the password when you generate the support bundle from the vSphere Client or using the `vm-support` command.
  The password recrypts core dumps that use internal keys to use keys that are based on the password. You can later use the password to decrypt any encrypted core dumps that might be included in the support bundle. Unencrypted core dumps and logs are not affected by using the password option.
- The password that you specify during `vm-support` bundle creation is not persisted in vSphere components. You are responsible for keeping track of passwords for support bundles.
- Before you change the host key, generate a `vm-support` bundle with a password. You can later use the password to access any core dumps that might have been encrypted with the old host key.

Key Lifecycle Management Best Practices

Implement best practices that guarantee key server availability and monitor keys on the key server.

- You are responsible for having policies in place that guarantee key server availability.
  If the key server is not available, virtual machine operations that require that vCenter Server request the key from the key server are not possible. That means running virtual machines continue to run, and you can power on, power off,

and reconfigure those virtual machines. However, you cannot relocate the virtual machine to a host that does not have the key information.

Most key server solutions include high availability features. You can use the vSphere Client or the API to specify a key provider and the associated key servers.

Note: Starting in version 7.0 Update 2, encrypted virtual machines and virtual TPMs can continue to function even when the key server is temporarily offline or unavailable. The ESXi hosts can persist the encryption keys to continue encryption and vTPM operations. See Key Persistence Overview.

- You are responsible for keeping track of keys and for performing remediation if keys for existing virtual machines are not in the Active state.

  The KMIP standard defines the following states for keys.

  - Pre-Active
  - Active
  - Deactivated
  - Compromised
  - Destroyed
  - Destroyed Compromised

  vSphere Virtual Machine Encryption uses only Active keys for encryption. If a key is Pre-Active, vSphere Virtual Machine Encryption activates it. If the key state is Deactivated, Compromised, Destroyed, Destroyed Compromised, you cannot encrypt a virtual machine or disk with that key.

  For keys that are in other states, virtual machines using those keys continue to work. Whether a clone or migration operation succeeds depends on whether they key is already on the host.

  - If the key is on the destination host, the operation succeeds even if the key is not Active on the key server.
  - If the required virtual machine and virtual disk keys are not on the destination host, vCenter Server has to fetch the keys from the key server. If the key state is Deactivated, Compromised, Destroyed, or Destroyed Compromised, vCenter Server displays an error and the operation does not succeed.

  A clone or migration operation succeeds if the key is already on the host. The operation fails if vCenter Server has to pull the keys from the key server.

  If a key is not Active, perform a rekey operation using the API. See the *vSphere Web Services SDK Programming Guide*.

- Develop key rotation policies so that keys are retired and rolled over after a specific time.
  - Trusted key provider: Change the primary key of a trusted key provider.
  - vSphere Native Key Provider: Change the `key_id` of a vSphere Native Key Provider.

Backup and Restore Best Practices

Set up policies on backup and restore operations.

- Not all backup architectures are supported. See Virtual Machine Encryption Interoperability.
- Set up policies for restore operations. Because backup is always in cleartext, plan to encrypt virtual machines right after restore is finished. You can specify that the virtual machine is encrypted as part of the restore operation. If possible, encrypt virtual machine as part of the restore process to avoid exposing sensitive information. To change the encryption policy for any disks that are associated with the virtual machine, change the storage policy for the disk.
- Because the VM home files are encrypted, ensure that the encryption keys are available at the time of a restore.

Performance Best Practices

- Encryption performance depends on the CPU and storage speed.
- Encrypting existing virtual machines is more time consuming than encrypting a virtual machine during creation. Encrypt a virtual machine when you create it if possible.

Storage Policy Best Practices

Do not modify the bundled VM Encryption sample storage policy. Instead, clone the policy and edit the clone.

Note: No automated way of returning VM Encryption Policy to its original settings exists.

See the *vSphere Storage* documentation for details customizing storage policies.

Removing Encryption Keys Best Practices

To ensure that encryption keys are removed from a cluster, after deleting, unregistering, or moving the encrypted virtual machine to another vCenter Server, reboot the ESXi hosts in the cluster.

Virtual Machine Encryption Caveats

Review Virtual Machine Encryption caveats to avoid problems later.

To understand which devices and features cannot be used with Virtual Machine Encryption, see Virtual Machine Encryption Interoperability.

Limitations

Consider the following caveats when you plan your virtual machine encryption strategy.

- When you clone an encrypted virtual machine or perform a Storage vMotion operation, you can attempt to change the disk format. Such conversions do not always succeed. For example, if you clone a virtual machine and attempt to change the disk format from lazy-zeroed thick format to thin format, the virtual machine disk keeps the lazy-zeroed thick format.
- When you detach a disk from a virtual machine, the storage policy information for the virtual disk is not retained.
  - If the virtual disk is encrypted, you must explicitly set the storage policy to VM Encryption Policy or to a storage policy that includes encryption.
  - If the virtual disk is not encrypted, you can change the storage policy when you add the disk to a virtual machine.

  See Virtual Disk Encryption for details.
- Decrypt core dumps before moving a virtual machine to a different cluster.

  The vCenter Server does not store KMS keys but only tracks the key IDs. As a result, vCenter Server does not store the ESXi host key persistently.

  Under certain circumstances, for example, when you move the ESXi host to a different cluster and reboot the host, vCenter Server assigns a new host key to the host. You cannot decrypt any existing core dumps with the new host key.
- OVF Export is not supported for an encrypted virtual machine.
- Using the VMware Host Client to register an encrypted virtual machine is not supported.

Virtual Machine Locked State

If the virtual machine key or one or more of the virtual disk keys are missing, the virtual machine enters a locked state. In a locked state, you cannot perform virtual machine operations.

- When you encrypt both a virtual machine and its disks from the vSphere Client, the same key is used for both.
- When you perform the encryption using the API, you can use different encryption keys for the virtual machine and for disks. In that case, if you attempt to power on a virtual machine, and one of the disk keys is missing, the power on operation fails. If you remove the virtual disk, you can power on the virtual machine.

See Resolve Missing Key Issues for troubleshooting suggestions.

Virtual Machine Encryption Interoperability

vSphere Virtual Machine Encryption has some limitations regarding devices and features that it can interoperate with.

The following limitations and remarks refer to using vSphere Virtual Machine Encryption. For similar information about using vSAN encryption, see the *Administering VMware vSAN* documentation.

Limitations on Certain Encryption Tasks

Some restrictions apply when performing certain tasks on an encrypted virtual machine.

- For most virtual machine encrypted operations, you must power off the virtual machine. You can clone an encrypted virtual machine and you can perform a shallow recrypt while the virtual machine is powered on.
  Note: Virtual machines configured with IDE controllers must be powered off to perform a shallow rekey operation.
- You cannot perform a deep recrypt on a virtual machine with snapshots. You can perform a shallow recrypt on a virtual machine with snapshots.

Virtual Trusted Platform Module Devices and vSphere Virtual Machine Encryption

A virtual Trusted Platform Module (vTPM) is a software-based representation of a physical Trusted Platform Module 2.0 chip. You can add a vTPM to either a new or an existing virtual machine. To add a vTPM to a virtual machine, you must configure a key provider in your vSphere environment. When you configure a vTPM, the virtual machine “home” files are encrypted (memory swap, NVRAM files, and so on). The disk files, or VMDK files, are not automatically encrypted. You can choose to add encryption explicitly for the virtual machine disks.

CAUTION: Cloning a virtual machine duplicates the entire virtual machine, including the virtual devices such as a vTPM. Information stored in the vTPM, including properties of the vTPM that software can use to determine a system’s identity, is also duplicated.

vSphere Virtual Machine Encryption and Suspended State and Snapshots

You can resume from a suspended state of an encrypted virtual machine, or revert to a memory snapshot of an encrypted machine. You can migrate an encrypted virtual machine with memory snapshot and suspended state between ESXi hosts.

vSphere Virtual Machine Encryption and IPv6

You can use vSphere Virtual Machine Encryption with pure IPv6 mode or in mixed mode. You can configure the key server with IPv6 addresses. You can configure both the vCenter Server and the key server with only IPv6 addresses.

Limitations on Cloning in vSphere Virtual Machine Encryption

Certain cloning features do not work with vSphere Virtual Machine Encryption.

- For a standard key provider, cloning is supported conditionally.
  – Full clones are supported. The clone inherits the parent encryption state including keys. You can encrypt the full clone, re-encrypt the full clone to use new keys, or decrypt the full clone.
  Linked clones are supported and the clone inherits the parent encryption state including keys. You cannot decrypt the linked clone or re-encrypt a linked clone with different keys.
  Note: Verify that other applications support linked clones. For example, VMware Horizon® 7 supports both full clones and instant clones, but not linked clones.
- For a trusted key provider or a vSphere Native Key Provider, cloning is supported, but encryption keys cannot be changed on clone. This behavior contrasts with standard encryption where you can change keys when creating a

clone. The following operations are not supported by vSphere Trust Authority or vSphere Native Key Provider during cloning of a virtual machine:
  - Cloning from an unencrypted virtual machine to an encrypted virtual machine
  - Cloning from an encrypted virtual machine and changing the encryption keys
  - Cloning from an encrypted virtual machine to an unencrypted virtual machine
- Instant clone is supported by all key provider types, but you cannot change encryption keys on clone.

Unsupported Disk Configurations with vSphere Virtual Machine Encryption

Certain types of virtual machine disk configurations are not supported with vSphere Virtual Machine Encryption.

- RDM (Raw Device Mapping). However, vSphere Virtual Volumes (vVols) are supported.
- Multi-writer or shared disks (MSCS, WSFC, or Oracle RAC). Encrypted virtual machine “home” files are supported for multi-writer disks. Encrypted virtual disks are not supported for multi-writer disks. If you attempt to select Multi-writer in the **Edit Settings** page of the virtual machine with encrypted virtual disks, the **OK** button is deactivated.

Miscellaneous Limitations in vSphere Virtual Machine Encryption

Other features that do not work with vSphere Virtual Machine Encryption include the following:

- vSphere ESXi Dump Collector
- Content Library
  - Content libraries support two types of templates, the OVF Template type and the VM Template type. You cannot export an encrypted virtual machine to the OVF Template type. The OVF Tool does not support encrypted virtual machines. You can create encrypted VM templates using the VM Template type. See the *vSphere Virtual Machine Administration* documentation.
- Software for backing up encrypted virtual disks must use the VMware vSphere Storage API - Data Protection (VADP) to either back up the disks in hot-add mode or NBD mode with SSL enabled. However, not all backup solutions that use VADP for virtual disk backup are supported. Check with your backup vendor for details.
  - VADP SAN transport mode solutions are not supported for backing up encrypted virtual disks.
  - VADP Hot-Add solutions are supported for encrypted virtual disks. The backup software must support encryption of the proxy VM that is used as part of the hot-add backup workflow. The vendor must have the privilege **Cryptographic Operations** > **Encrypt Virtual Machine**.
  - Backup solutions using the NBD-SSL transport modes are supported for backing up encrypted virtual disks. The vendor application must have the privilege **Cryptographic Operations** > **Direct Access**.
- You cannot send output from an encrypted virtual machine to a serial port or parallel port. Even if the configuration appears to succeed, output is sent to a file.
- vSphere Virtual Machine Encryption is not supported in VMware Cloud on AWS. See the *Managing the VMware Cloud on AWS Data Center* documentation.

Key Persistence Overview

In vSphere 7.0 Update 2 and later, encrypted virtual machines and virtual TPMs can continue to optionally function even when the key server is temporarily offline or unavailable. The ESXi hosts can persist the encryption keys to continue encryption and vTPM operations.

Before vSphere 7.0 Update 2, encrypted virtual machines and vTPMs require that the key server always is available to function. In vSphere 7.0 Update 2 and later, encrypted devices can function even when access to a key server is disrupted.

Starting in vSphere 7.0 Update 3, encrypted vSAN clusters can also function even when access to a key provider is disrupted.

Note: Key persistence is not necessary when using vSphere Native Key Provider. vSphere Native Key Provider is designed out-of-the-box to run without requiring access to a key server. See the following section, "Key Persistence and vSphere Native Key Provider."

Key Persistence on the ESXi Host

When using a standard key provider, the ESXi host relies on vCenter Server to manage the encryption keys. When using a trusted key provider, the ESXi host relies directly on the Trust Authority Hosts for keys, and vCenter Server is not involved.

Regardless of the type of key provider, the ESXi host obtains the keys initially and retains them in its key cache. If the ESXi host reboots, it loses its key cache. The ESXi host then requests the keys again, either from the key server (standard key provider), or the Trust Authority Hosts (trusted key provider). When the ESXi host tries to obtain keys and the key server is offline or unreachable, vTPMs and workload encryption cannot function. For edge-style deployments, in which a key server is typically not deployed on site, a loss of connectivity to a key server can cause unnecessary downtime for encrypted workloads.

In vSphere 7.0 Update 2 and later, encrypted workloads can continue to function even when the key server is offline or unreachable. If the ESXi host has a TPM, the encryption keys are persisted in the TPM across reboots. So, even if an ESXi host reboots, the host does not need to request encryption keys. Also, encryption and decryption operations can continue when the key server is unavailable, because the keys have persisted in the TPM. In essence, when either the key server or Trust Authority Hosts are unavailable, you can keep running encrypted workloads "key server free." Also, vTPMs can likewise continue to function even when the key server is unreachable.

Key Persistence and vSphere Native Key Provider

When using a vSphere Native Key Provider, vSphere generates encryption keys and no key server is required. The ESXi hosts get a Key Derivation Key (KDK), which is used to derive other keys. After receiving the KDK and generating other keys, the ESXi hosts do not need access to vCenter Server to do encryption operations. In essence, a vSphere Native Key Provider always runs "key server free."

The KDK persists on an ESXi host by default even after reboot, and even when vCenter Server is not available after the host reboots.

You can activate key persistence with vSphere Native Key Provider, but it is normally unnecessary. The ESXi hosts have complete access to vSphere Native Key Provider and so additional persistence of keys is redundant. One use case for activating key persistence with vSphere Native Key Provider is when you also have a standard key provider (external KMIP server) configured.

How Do You Set Up Key Persistence

To enable or disable key persistence, see Enable and Disable Key Persistence on an ESXi Host.

Configuring and Managing a Standard Key Provider

Using a standard key provider in your vSphere environment requires some preparation. After your environment is set up, you can create encrypted virtual machines and virtual disks and encrypt existing virtual machines and disks.

After your environment is set up for a standard key provider, you can use the vSphere Client to create encrypted virtual machines and virtual disks and encrypt existing virtual machines and disks. See Use Encryption in Your vSphere Environment.

You can perform additional tasks by using the API and by using the crypto-util CLI. See the *vSphere Web Services SDK Programming Guide* for the API documentation and the `crypto-util` command-line help for details about that tool.

Standard Key Provider Overview

You can use a standard key provider to perform virtual machine encryption tasks.

What Is a Standard Key Provider?

In vSphere, a standard key provider gets encryption keys directly from a key server, and the vCenter Server distributes the keys to the required ESXi hosts in a data center.

You can add separate standard key providers for different users and set the default standard key provider.

vSphere Standard Key Provider Requirements

- vSphere 6.5 or later
- An external key server (KMS)

The Key Management Server must support the Key Management Interoperability Protocol (KMIP) 1.1 standard. See the *vSphere Compatibility Matrixes* for details.

You can find information about VMware certified KMS vendors in the VMware Compatibility Guide under Platform and Compute. If you select Compatibility Guides, you can open the Key Management Server (KMS) compatibility documentation. This documentation is updated frequently.

Standard Key Provider Privileges

Standard key providers use the **Cryptographer.*** privileges. See Cryptographic Operations Privileges.

Set Up the Standard Key Provider

Before you can start with virtual machine encryption tasks, you must set up the standard key provider.

Setting up a standard key provider includes adding the key provider and establishing trust with the key server. When you add a key provider, you are prompted to make it the default. You can explicitly change the default key provider. vCenter Server provisions keys from the default key provider.

Note: What was previously called a Key Management Server cluster in vSphere 6.5 and 6.7 is now called a key provider.

Add a Standard Key Provider Using the vSphere Client

You can add a standard key provider to your vCenter Server system from the vSphere Client or by using the public API.

- Verify that the key server (KMS) is in the *VMware Compatibility Guide for Key Management Servers (KMS)* and is KMIP 1.1 compliant, and that it can be a symmetric key foundry and server.
- Verify that you have the required privileges: **Cryptographic operations** > **Manage key servers**.
- Ensure that the key server is highly available. Loss of connection to the key server, such as during a power outage or a disaster recovery event, renders encrypted virtual machines inaccessible.

  Note: Starting in vSphere 7.0 Update 2, encrypted virtual machines and virtual TPMs can continue to function even when the key server is temporarily offline or unavailable. See Key Persistence Overview.
- Consider your infrastructure's dependencies on the key server carefully. Some KMS solutions are delivered as virtual appliances, making it possible to create a dependency loop or other availability problem with poor placement of the KMS appliance.

The vSphere Client enables you to add a standard key provider to your vCenter Server system, and establish trust between the key server and vCenter Server.

- You can add multiple key servers from the same vendor.
- If your environment supports solutions from different vendors, you can add multiple key providers.
- If your environment includes multiple key providers, and you delete the default key provider, you must set another default explicitly.
- You can configure the key server with IPv6 addresses.
  - Both the vCenter Server system and the key server can be configured with only IPv6 addresses.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure**, and under **Security** click **Key Providers**.
4. Click **Add Standard Key Provider** and enter the key provider information.

Option	Value
Name	Name for the key provider. Each logical key provider, regardless of its type (Standard, Trusted, and Native Key Provider), must have a unique name across all vCenter Server systems. For more information, see Key Provider Naming.
KMS	Alias for the key server (KMS).
Address	IP address or FQDN of the key server.
Port	Port on which vCenter Server connects to the key server.
Proxy server	Optional proxy server address for connecting to the key server.
Proxy port	Optional proxy port for connecting to the key server.
Username	Some key server vendors allow users to isolate encryption keys that are used by different users or groups by specifying a user name and password. Specify a user name only if your key server supports this functionality, and if you intend to use it.
Password	Some key server vendors allow users to isolate encryption keys that are used by different users or groups by specifying a user name and password. Specify a password only if your key server supports this functionality, and if you intend to use it.

   You can click **Add KMS** to add more key servers.
5. Click **Add Key Provider**.
6. Click **Trust**.
   vCenter Server adds the key provider and displays the status as Connected.

See Establish a Standard Key Provider Trusted Connection by Exchanging Certificates.

Establish a Standard Key Provider Trusted Connection by Exchanging Certificates

After you add the standard key provider to the vCenter Server system, you can establish a trusted connection. The exact process depends on the certificates that the key provider accepts, and on your company policy.

Add the standard key provider.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider.
   The KMS for the key provider is displayed.
4. Select the KMS.
5. From the **Establish Trust** drop-down menu, select **Make KMS trust vCenter**.
6. Select the option appropriate for your server and follow the steps.

Option	See
vCenter Server Root CA certificate	Use the Root CA Certificate Option to Establish a Standard Key Provider Trusted Connection.
vCenter Server Certificate	Use the Certificate Option to Establish a Standard Key Provider Trusted Connection.
Upload certificate and private key	Use the Upload Certificate and Private Key Option to Establish a Standard Key Provider Trusted Connection.
New Certificate Signing Request	Use the New Certificate Signing Request Option to Establish a Standard Key Provider Trusted Connection.

Use the Root CA Certificate Option to Establish a Standard Key Provider Trusted Connection

Some Key Management Server (KMS) vendors require that you upload your root CA certificate to the KMS. All certificates that are signed by your root CA are then trusted by this KMS.

The root CA certificate that vSphere Virtual Machine Encryption uses is a self-signed certificate that is stored in a separate store in the VMware Endpoint Certificate Store (VECS) on the vCenter Server system.

Note: Generate a root CA certificate only if you want to replace existing certificates. If you do, other certificates that are signed by that root CA become invalid. You can generate a new root CA certificate as part of this workflow.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider with which you want to establish a trusted connection.
   The KMS for the key provider is displayed.
4. From the **Establish Trust** drop-down menu, select **Make KMS trust vCenter**.
5. Select **vCenter Root CA Certificate** and click **Next**.
   The Download Root CA Certificate dialog box is populated with the root certificate that vCenter Server uses for encryption. This certificate is stored in VECS.
6. Copy the certificate to the clipboard or download the certificate as a file.
7. Follow the instructions from your KMS vendor to upload the certificate to their system.

   Note: Some KMS vendors require that the KMS vendor restarts the KMS to pick up the root certificate that you upload.

Finalize the certificate exchange. See Finish the Trust Setup for a Standard Key Provider.

Use the Certificate Option to Establish a Standard Key Provider Trusted Connection

Some Key Management Server (KMS) vendors require that you upload the vCenter Server certificate to the KMS. After the upload, the KMS accepts traffic that comes from a system with that certificate.

vCenter Server generates a certificate to protect connections with the KMS. The certificate is stored in a separate key store in the VMware Endpoint Certificate Store (VECS) on the vCenter Server system.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider with which you want to establish a trusted connection.
   The KMS for the key provider is displayed.
4. From the **Establish Trust** drop-down menu, select **Make KMS trust vCenter**.
5. Select **vCenter Certificate** and click **Next**.
   The Download Certificate dialog box is populated with the root certificate that vCenter Server uses for encryption. This certificate is stored in VECS.

   Note: Do not generate a new certificate unless you want to replace existing certificates.
6. Copy the certificate to the clipboard or download it as a file.
7. Follow the instructions from your KMS vendor to upload the certificate to the KMS.

Finalize the trust relationship. See Finish the Trust Setup for a Standard Key Provider.

Use the Upload Certificate and Private Key Option to Establish a Standard Key Provider Trusted Connection

Some Key Management Server (KMS) vendors require that you upload the KMS server certificate and private key to the vCenter Server system.

- Request a certificate and private key from the KMS vendor. The files are X509 files in PEM format.

Some KMS vendors generate a certificate and private key for the connection and make them available to you. After you upload the files, the KMS trusts your vCenter Server instance.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider with which you want to establish a trusted connection.
   The KMS for the key provider is displayed.
4. From the **Establish Trust** drop-down menu, select **Make KMS trust vCenter**.
5. Select **KMS certificate and private key** and click **Next**.
6. Paste the certificate that you received from the KMS vendor into the top text box or click **Upload a File** to upload the certificate file.
7. Paste the key file into the bottom text box or click **Upload a File** to upload the key file.
8. Click **Establish Trust**.

Finalize the trust relationship. See Finish the Trust Setup for a Standard Key Provider.

Use the New Certificate Signing Request Option to Establish a Standard Key Provider Trusted Connection

Some Key Management Server (KMS) vendors require that vCenter Server generate a Certificate Signing Request (CSR) and send that CSR to the KMS. The KMS signs the CSR and returns the signed certificate. You can upload the signed certificate to vCenter Server.

Using the **New Certificate Signing Request** option is a two-step process. First you generate the CSR and send it to the KMS vendor. Then you upload the signed certificate that you receive from the KMS vendor to vCenter Server.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider with which you want to establish a trusted connection.
   The KMS for the key provider is displayed.
4. From the **Establish Trust** drop-down menu, select **Make KMS trust vCenter**.
5. Select **New Certificate Signing Request (CSR)** and click **Next**.
6. In the dialog box, copy the full certificate in the text box to the clipboard or download it as a file.
   Use the **Generate new CSR** button in the dialog box only if you explicitly want to generate a CSR. Using that option makes any signed certificates that are based on the old CSR invalid.
7. Follow the instructions from your KMS vendor to submit the CSR.
8. When you receive the signed certificate from the KMS vendor, click **Key Providers** again, select the key provider, and from the **Establish Trust** drop-down menu, select **Upload Signed CSR Certificate**.
9. Paste the signed certificate into the bottom text box or click **Upload File** and upload the file, and click **Upload**.

Finalize the trust relationship. See Finish the Trust Setup for a Standard Key Provider.

Set the Default Key Provider

You must set the default key provider if you do not make the first key provider the default, or if your environment uses multiple key providers and you remove the default one.

As a best practice, verify that the Connection Status in the **Key Providers** tab shows Connected and a green check mark.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider.
4. Click **Make Default**.
   A confirmation dialog box appears.
5. Click **Make Default**.
   The key provider displays as the current default.

Finish the Trust Setup for a Standard Key Provider

Unless the **Add Standard Key Provider** dialog box prompted you to trust the KMS, you must explicitly establish trust after certificate exchange is complete.

You can complete the trust setup, that is, make vCenter Server trust the KMS, either by trusting the KMS or by uploading a KMS certificate. You have two options:

- Trust the certificate explicitly by using the **Upload KMS certificate** option.
- Upload a KMS leaf certificate or the KMS CA certificate to vCenter Server by using the **Make vCenter Trust KMS** option.

Note: If you upload the root CA certificate or the intermediate CA certificate, vCenter Server trusts all certificates that are signed by that CA. For strong security, upload a leaf certificate or an intermediate CA certificate that the KMS vendor controls.

1. Navigate to the .
2. Click **Configure** and select **Key Providers** under **Security**.
3. Select the key provider with which you want to establish a trusted connection.
   The KMS for the key provider is displayed.
4. Select the KMS.
5. Select one of the following options from the **Establish Trust** drop-down menu.

Option	Action
Make vCenter Trust KMS	In the dialog box that appears, click **Trust**.
Upload KMS certificate	1. In the dialog box that appears, either paste in the certificate, or click **Upload a file** and browse to the certificate file. 2. Click **Upload**.

Set Up Separate Key Providers for Different Users

You can set up your environment with different key providers for different users of the same KMS instance. Having multiple key providers is helpful, for example, if you want to grant different departments in your company access to different sets of encryption keys.

Set up the connection with the KMS.

You can use multiple key providers for the same KMS to separate keys. Having separate sets of keys is essential for use cases like different BUs or different customers.

Note: Not all KMS vendors support multiple users.

1. Create two users with corresponding user names and passwords, for example C1 and C2, on the KMS.
2. Log in to vCenter Server and create the first key provider.
3. When prompted for a user name and password, give information that is unique to the first user.
4. Create a second key provider and add the same KMS, but use the second user name and password (C2).

The two key providers have independent connections to the KMS and use a different set of keys.

Delete a Standard Key Provider

You can use the vSphere Client to delete a standard key provider from vCenter Server.

Required privilege: **Cryptographic operations** > **Manage key servers**

Before you delete a standard key provider, rekey any encrypted virtual machines and datastores that were encrypted using that key provider to another key provider. See Rekey an Encrypted Virtual Machine Using the vSphere Client.

In addition, maintain a backup of the standard key provider in case you must rekey an encrypted virtual machine after deleting the key provider.

After you delete a standard key provider, virtual machines that have vTPMs or that are encrypted continue to run. If you reboot the ESXi host, its encrypted virtual machines enter a locked state. After you unregister these virtual machines,

they enter a locked state when you try to re-register them. The only way to unlock the virtual machines is to restore the previous standard key provider.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure**, and under **Security** click **Key Providers**.
4. Select the standard key provider you want to delete.
5. Click **Delete**.
6. Read the warning message and slide the slider all the way to the right.
7. Click **Delete**.

The standard key provider is removed from the vCenter Server.

Configuring and Managing vSphere Native Key Provider

Using a VMware vSphere®Native Key Provider™ in your vSphere environment requires some preparation. After you configure vSphere Native Key Provider, you can create virtual Trusted Platform Modules (vTPMs) on your virtual machines.

After you set up your environment for vSphere Native Key Provider, you can use the vSphere Client and API to create vTPMs. If you purchase the VMware vSphere®Enterprise Plus Edition™, you can also encrypt virtual machines and virtual disks, and encrypt existing virtual machines and disks.

vSphere Native Key Provider Overview

In vSphere 7.0 Update 2 and later, you can use the built-in vSphere Native Key Provider to enable encryption technologies, such as virtual TPMs (vTPM).

vSphere Native Key Provider is included in all vSphere editions and does not require an external key server (also called a Key Management Server (KMS) in the industry). You can also use vSphere Native Key Provider for vSphere Virtual Machine Encryption, but you must purchase the VMware vSphere®Enterprise Plus Edition™.

What Is vSphere Native Key Provider

With a standard key provider or trusted key provider, you must configure an external key server. In a standard key provider setup, vCenter Server fetches the keys from the external key server and distributes them to the ESXi hosts. In a trusted key provider (vSphere Trust Authority) setup, the trusted ESXi hosts fetch the keys directly.

With vSphere Native Key Provider, you no longer need an external key server. vCenter Server generates a primary key, called the Key Derivation Key (KDK), and pushes it to all ESXi hosts in the cluster. The ESXi hosts then generate data encryption keys (even when not connected to vCenter Server) to enable security functionality such as vTPMs. vTPM functionality is included in all vSphere editions. To use vSphere Native Key Provider for vSphere Virtual Machine Encryption, you must have purchased the vSphere Enterprise Plus Edition. vSphere Native Key Provider can coexist with an existing key server infrastructure.

vSphere Native Key Provider:

- Enables the use of vTPMs, vSphere Virtual Machine Encryption, and vSAN Data at Rest Encryption, when you do not require or want an external key server.

- Works only with VMware infrastructure products.
- Does not provide external interoperability, KMIP support, hardware security modules, or other features that a traditional, third-party, external key server can offer for interoperability or regulatory compliance. If your organization requires this functionality for non-VMware products and components, install a traditional, third-party key server.
- Helps address the needs of organizations that either cannot use, or do not want not to use, an external key server.
- Improves data sanitization and system reuse practices by enabling earlier use of encryption technologies on media that is difficult to sanitize, such as flash and SSD.
- Provides a transition path between key providers. vSphere Native Key Provider is compatible with the VMware standard key provider and the vSphere Trust Authority trusted key provider.
- Works with multiple vCenter Server systems using an Enhanced Linked Mode configuration or a vCenter Server High Availability configuration.
- Can be used to enable vTPM in all editions of vSphere, and encrypt virtual machines with the purchase of the vSphere Enterprise Plus Edition that includes vSphere Virtual Machine Encryption. vSphere Virtual Machine Encryption works with vSphere Native Key Provider as it does with VMware standard and trusted key providers.
- Can be used to enable vSAN Data at Rest Encryption with the use of an appropriate vSAN license.
- Can use a Trusted Platform Module (TPM) 2.0 to increase security when one is installed in an ESXi host. You can also configure vSphere Native Key Provider to be available only to hosts where a TPM 2.0 is installed. If you use a TPM, it must be TPM 2.0. vSphere Native Key Provider does not support TPM 1.2.

Note: An ESXi host does not require a TPM 2.0 to use a vSphere Native Key Provider. However, a TPM 2.0 does provide enhanced security.

As with all security solutions, consider the system design, implementation considerations, and tradeoffs of using Native Key Provider. For example, ESXi key persistence avoids the dependency on a key server always being available. However, because key persistence stores the Native Key Provider cryptographic information on the clustered hosts, you still are at risk if malicious actors steal the ESXi hosts themselves. Because environments differ, assess and implement your security controls in accordance with your organization's regulatory and security needs, operational requirements, and tolerance for risk.

For more overview information about vSphere Native Key Provider, see https://core.vmware.com/native-key-provider.

vSphere Native Key Provider Requirements

To use vSphere Native Key Provider, you must:

- Ensure that both the vCenter Server system and ESXi hosts are running vSphere 7.0 Update 2 or later.
- Configure the ESXi hosts in a cluster.
- Configure the vCenter Server file-based backup and restore, and store the backups securely as they contain the Key Derivation Key. See the topic on vCenter Server backup and restore in the *vCenter Server Installation and Setup* documentation.
- While not required, as a best practice, use ESXi hosts that are as identical as possible, including TPMs. Cluster management and feature enablement is much easier when cluster hosts are identical.

To perform vSphere Virtual Machine Encryption or vSAN encryption using vSphere Native Key Provider, you must purchase the edition of those products containing the appropriate license.

vSphere Native Key Provider and Enhanced Linked Mode

You can configure a single vSphere Native Key Provider that is shareable across vCenter Server systems configured in an Enhanced Linked Mode configuration. The high-level steps in this scenario are:

1. Creating the vSphere Native Key Provider on one of the vCenter Server systems
2. Backing up the Native Key Provider on the vCenter Server on which it was created
3. Exporting the Native Key Provider

4. Restoring the Native Key Provider to the other vCenter Server systems in the Enhanced Link Mode configuration (see Restore a vSphere Native Key Provider Using the vSphere Client)

vSphere Native Key Provider Privileges

As with standard and trusted key providers, vSphere Native Key Provider uses the **Cryptographer.*** privileges. In addition, vSphere Native Key Provider uses the **Cryptographer.ReadKeyServersInfo** privilege, which is specific to vSphere Native Key Providers, to list vSphere Native Key Providers. See Cryptographic Operations Privileges.

vSphere Native Key Provider Alarms

You must back up a vSphere Native Key Provider. When a vSphere Native Key Provider is not backed up, vCenter Server generates an alarm. When you back up the vSphere Native Key Provider for which an alarm was generated, vCenter Server resets the alarm. By default, vCenter Server checks for backed-up vSphere Native Key Providers once a day. You can change the checking interval by modifying the `vpxd.KMS.backupCheckInterval` option.

vSphere Native Key Provider Periodic Remediation Check

vCenter Server checks periodically that the vSphere Native Key Provider configuration on vCenter Server and ESXi hosts matches. When a host state changes, for example, when you add a host to the cluster, the key provider configuration on the cluster drifts away from the configuration on the host. If the configuration (keyID) differs on the host, vCenter Server updates the configuration of the host automatically. No manual intervention is required.

By default, vCenter Server checks the configuration every five minutes. You can modify the interval by using the `vpxd.KMS.remediationInterval` option.

Using vSphere Native Key Provider with a Disaster Recovery Site

You can use vSphere Native Key Provider with a backup disaster recovery site. Importing the vSphere Native Key Provider backup from the primary vCenter Server to the vCenter Server backup at the disaster recovery site enables that cluster to decrypt and run your encrypted virtual machines.

Always test your DR solution. Never assume that your solution works without trying a recovery. Ensure that a copy of the vSphere Native Key Provider backup is also available to your DR site.

Unsupported Features in vSphere Native Key Provider

Currently, vSphere Native Key Provider does not support the following:

- First Class Disk (FCD) encryption

vSphere Native Key Provider Process Flows

Understanding vSphere Native Key Provider process flows is essential to learning how to configure and manage your vSphere Native Key Provider.

You can use the built-in vSphere Native Key Provider to power encryption-based virtual TPMs (vTPM). vSphere Native Key Provider is included in all vSphere editions and does not require an external key server (KMS). To use vSphere Native Key Provider for vSphere Virtual Machine Encryption, you must purchase the vSphere Enterprise+ edition.

Configuring vSphere Native Key Provider

Configuring vSphere Native Key Provider involves these basic operations:

1. A user with the appropriate administrative privileges uses the vSphere Client to create a vSphere Native Key Provider on a vCenter Server.

2. The vCenter Server then configures the vSphere Native Key Provider for all clusters of ESXi hosts.
   In this step, vCenter Server pushes a primary key to all ESXi hosts in the cluster. Likewise, if you update or delete a vSphere Native Key Provider, the change is pushed to the hosts in the cluster.
3. Users with the appropriate cryptographic privileges create vTPMs and encrypted virtual machines (provided you have purchased the vSphere Enterprise+ edition).
   See Securing Virtual Machines with Virtual Trusted Platform Module and Use Encryption in Your vSphere Environment.

vSphere Native Key Provider Encryption Process Flow

To understand how different components interact to perform an encryption task using vSphere Native Key Provider, see Encryption Process Flow.

Configure a vSphere Native Key Provider

Before you can start with encryption tasks, you must configure a vSphere Native Key Provider on vCenter Server.

Required privilege: **Cryptographic operations** > **Manage key servers**

vSphere 7.0 Update 2 and later includes a key provider called vSphere Native Key Provider. vSphere Native Key Provider enables encryption-related functionality without requiring an external key server (KMS). Initially, vCenter Server is not configured with a vSphere Native Key Provider. You must manually configure a vSphere Native Key Provider.

An ESXi host does not require a TPM 2.0 to use a vSphere Native Key Provider. However, a TPM 2.0 does provide enhanced security.

Note: When you configure vSphere Native Key Provider, the key providers are available on all clusters for the vCenter Server on which you configure them. As a result, all hosts attached to the vCenter Server have access to all the vSphere Native Key Providers that you configure.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure**, and under **Security** click **Key Providers**.
4. Click **Add** then click **Add Native Key Provider**.
5. Enter a name for the vSphere Native Key Provider.

   Each logical key provider, regardless of its type (Standard, Trusted, and Native Key Provider), must have a unique name across all vCenter Server systems.

   For more information, see Key Provider Naming.
6. If you want this vSphere Native Key Provider to be used only by hosts with a TPM 2.0, select the **Use key provider only with TPM protected ESXi hosts** check box.
   If enabled, the vSphere Native Key Provider is available only on hosts with a TPM 2.0.
7. Click **Add Key Provider**.

   Note: It takes about five minutes for all the clustered ESXi hosts in a data center to get the key provider, and for the vCenter Server to update its cache. Because of the way the information is propagated, you might have to wait for a few minutes to use the key provider for key operations on some of the hosts.

The vSphere Native Key Provider is added and appears in the **Key Provider** pane. At this point, the vSphere Native Key Provider is not backed up. You must back up the vSphere Native Key Provider before you can use it.

See Back up a vSphere Native Key Provider.

Back up a vSphere Native Key Provider

In case you must restore the key provider configuration, backing up a vSphere Native Key Provider is required as part of a disaster recovery scenario. You can use the vSphere Client, PowerCLI, or API to back up the vSphere Native Key Provider.

Required privilege: **Cryptographic operations** > **Manage key servers**

Note: In an Enhanced Link Mode configuration, you must perform the backup on the vCenter Server that the key provider belongs to.

vSphere Native Key Provider is backed up as part of the vCenter Server file-based backup. However, you must back up the vSphere Native Key Provider at least once before you can use it. When you create a vSphere Native Key Provider, it is not backed up.

A backup is necessary in case you must restore the configuration. To restore a vSphere Native Key Provider, see Restore a vSphere Native Key Provider Using the vSphere Client.

Keep the backup file in a secure location. You can password-protect the backup when you create it. The backup file is in PKCS#12 format.

vCenter Server creates an alarm if a vSphere Native Key Provider has not been backed up. You can acknowledge the alarm, but it reappears every 24 hours until you have backed up the vSphere Native Key Provider.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure**, and under **Security** click **Key Providers**.
4. Select the vSphere Native Key Provider you want to back up.
   A status of "Not backed up" appears for key providers that you have not backed up.
5. Click **Back Up**.
6. To password-protect the backup, check the **Protect Native Key Provider data with password** box.
   a) Enter a password and save it in a secure location.
   b) Check the **I have saved the password in a secure place** box, indicating that you have saved the password to a secure place.
7. Click **Back Up Key Provider**.
   The backup file is in PKCS#12 format.
8. Save the backup file in a secure location.

The status of the vSphere Native Key Provider changes from Not Backed Up, to Warning, to Active. Warning indicates that the vCenter Server is still pushing the information to all the ESXi hosts in the data center. Active means that the information has been pushed to all the hosts.

To add vTPMs to your virtual machines, see Securing Virtual Machines with Virtual Trusted Platform Module. To encrypt virtual machines, see Use Encryption in Your vSphere Environment.

Recovering a vSphere Native Key Provider

You can recover the vSphere Native Key Provider either through the vSphere Client or from the vCenter Server Appliance Backup.

When necessary, you can recover a vSphere Native Key Provider in the following ways.

1. If you do not need to rebuild your vCenter Server Appliance, use the vSphere Client to restore the key provider. See Restore a vSphere Native Key Provider Using the vSphere Client.

2. If you must rebuild your vCenter Server Appliance, you must restore the key provider from your vCenter Server Appliance Backup. When you perform a vCenter Server Appliance Backup, it saves the Native Key Provider. See https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html for information about restoring the vCenter Server Appliance from backup.

Restore a vSphere Native Key Provider Using the vSphere Client

You can use the vSphere Client to restore the vSphere Native Key Provider.

- Required privilege: **Cryptographic operations** > **Manage key servers**
- The key provider backup file.
- The password for the key provider file, if you entered one when you backed up the key provider.

You can restore a vSphere Native Key Provider in case it was accidentally deleted or if you must perform a disaster recovery.

When you restore a vSphere Native Key Provider, you do not need to back up the key provider again. The initial backup suffices. Continue to maintain the backup file in a secure location.

Note: You can also use this task to configure vSphere Native Key Provider for vCenter Server systems in an Enhanced Linked Mode configuration. After you create the vSphere Native Key Provider on one vCenter Server system in the Enhanced Linked Mode configuration, use the **Restore** function to import the encrypted key file to the other ELM-connected vCenter Server systems.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure**, and under **Security** click **Key Providers**.
4. Select the vSphere Native Key Provider and click **Restore**.
5. Browse to the file location and select the backup encrypted key file.
   The file was saved in PKCS#12 format.
6. Optional: If the file is password protected, enter the password.
7. Click **Next**.
8. Optional: If you decided to use this key provider only with TPM-protected ESXi hosts, select the check box.
9. Click **Finish**.

The vSphere Native Key Provider is imported to the vCenter Server. To use the vSphere Native Key Provider for encryption tasks, ensure that you first select it in the **Key Provider** pane and click **Set as Default**.

Update a vSphere Native Key Provider

As part of your regular key rotation plans, you can use PowerCLI to update a vSphere Native Key Provider.

- Required privilege: **Cryptographic operations** > **Manage key servers**
- PowerCLI 12.3.0

If you have a policy for key rotation, you can update the vSphere Native Key Provider and rekey the virtual machines that you encrypted with that key provider. You must use PowerCLI to update the vSphere Native Key Provider. You can also

rekey the encrypted virtual machines without updating the key provider. In this case, only the virtual machine keys are changed. To rekey a virtual machine, see Rekey an Encrypted Virtual Machine Using the vSphere Client.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as an administrator user to the vCenter Server where you configured the vSphere Native Key Provider that you want to update.

   ```
   Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
   ```

2. To get your vSphere Native Key Provider names, run the `Get-KeyProvider` cmdlet with the optional Type parameter.

   ```
   Get-KeyProvider -Type NativeKeyProvider
   ```

3. To update the key provider, run the `Set-KeyProvider` cmdlet, specifying your key provider name and GUID.

   You can generate a GUID to use by running the `New-Guid` cmdlet.

   ```
   Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
   ```

   A warning appears about backing up the configuration.

4. To back up the key provider, run the `Export-KeyProvider` cmdlet.

   ```
   Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
   ```

   You can also back up the key provider using the vSphere Client. See Back up a vSphere Native Key Provider.

When a key provider is updated, its status changes to Not Backed Up. After you back up the key provider, its status changes to Active.

Delete a vSphere Native Key Provider

You can delete a vSphere Native Key Provider from vCenter Server.

Required privilege: **Cryptographic operations** > **Manage key servers**

Before you delete a vSphere Native Key Provider, rekey any encrypted virtual machines and datastores that were encrypted using that key provider to another key provider. See Rekey an Encrypted Virtual Machine Using the vSphere Client.

In addition, maintain a backup of the vSphere Native Key Provider in case you must rekey an encrypted virtual machine after deleting the key provider.

After you delete a vSphere Native Key Provider, virtual machines that have vTPMs or that are encrypted continue to run. If you reboot the ESXi host, its encrypted virtual machines enter a locked state. After you unregister these virtual machines, they enter a locked state when you try to re-register them. The only way to unlock the virtual machines is to restore the previous vSphere Native Key Provider.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the vCenter Server instance.
3. Click **Configure**, and under **Security** click **Key Providers**.
4. Select the key provider you want to delete.
5. Click **Delete**.
6. Read the warning message and slide the slider all the way to the right.
7. Click **Delete**.

The vSphere Native Key Provider is removed from the vCenter Server.

vSphere Trust Authority

With vSphere 7.0 and later, you can take advantage of VMware®vSphere Trust Authority™. vSphere Trust Authority is a foundational technology that enhances workload security. vSphere Trust Authority establishes a greater level of trust in your organization by associating an ESXi host's hardware root of trust to the workload itself.

vSphere Trust Authority Concepts and Features

vSphere Trust Authority secures your SDDC against malicious attacks by extending the trustworthiness of a trusted computing base to your organization's entire computing infrastructure. vSphere Trust Authority uses remote attestation and controlled access to advanced cryptographic capabilities.

vSphere Trust Authority is a set of services that satisfies high security requirements. With vSphere Trust Authority, you can set up and maintain a secure infrastructure. You can ensure that sensitive workloads run only on ESXi hosts proven to have booted authentic software.

How vSphere Trust Authority Protects Your Environment

You configure vSphere Trust Authority services to attest your ESXi hosts, which then become capable of performing trusted cryptographic operations.

vSphere Trust Authority uses remote attestation for ESXi hosts to prove the authenticity of their booted software. Attestation verifies that the ESXi hosts are running authentic VMware software, or VMware-signed partner software. Attestation relies on measurements that are rooted in a Trusted Platform Module (TPM) 2.0 chip installed in the ESXi host. In vSphere Trust Authority, an ESXi can access encryption keys and perform cryptographic operations only after it has been attested.

vSphere Trust Authority Glossary

vSphere Trust Authority introduces specific terms and definitions that are important to understand.

Table 256: vSphere Trust Authority Glossary

Term	Definition
VMware vSphere®Trust Authority™	Specifies a set of services that enables a Trusted Infrastructure. It is responsible for ensuring that ESXi hosts are running trusted software and for releasing encryption keys only to trusted ESXi hosts.
vSphere Trust Authority Components	The vSphere Trust Authority components are: • Attestation Service • Key Provider Service
Attestation Service	Attests the state of a remote ESXi host. Uses TPM 2.0 to establish a hardware root of trust, and verifies software measurements against a list of administrator approved ESXi versions.
Key Provider Service	Encapsulates one or more key servers and exposes Trusted Key Providers that can be specified when encrypting virtual machines. Currently, key servers are limited to the KMIP protocol.
Trusted Infrastructure	A Trusted Infrastructure consists of: • A Trust Authority vCenter Server • A Workload vCenter Server • At least one vSphere Trust Authority Cluster (configured as part of the Trust Authority vCenter Server)

Term	Definition
	• At least one Trusted Cluster (configured as part of the Workload vCenter Server) • Encrypted workload virtual machines running in the Trusted Cluster • At least one KMIP-compliant key management server **Note:** You must use separate vCenter Server systems for the Trust Authority Cluster and the Trusted Cluster.
Trust Authority Cluster	Consists of a vCenter Server cluster of ESXi hosts that run the vSphere Trust Authority components (the Attestation Service and the Key Provider Service).
Trust Authority Host	An ESXi host running vSphere Trust Authority components (the Attestation Service and the Key Provider Service).
Trusted Cluster	Consists of a vCenter Server cluster of Trusted ESXi hosts that are remotely attested by the Trust Authority Cluster. Although not strictly required, a configured Key Provider Service greatly increases the value provided by a Trusted Cluster.
Trusted Host	An ESXi host whose software has been validated by the Trust Authority Cluster Attestation Service. This host runs workload virtual machines that can be encrypted using Key Providers published by the Trust Authority Cluster Key Provider Service.
vSphere Encryption for Virtual Machines	With vSphere Virtual Machine Encryption, you can create encrypted virtual machines and encrypt existing virtual machines. • Starting in vSphere 6.5, vCenter Server requests keys from an external key server. The key server generates and stores the keys, and passes them to vCenter Server for distribution. • Starting in vSphere 7.0, the trusted connection can be set up between vSphere Trust Authority and a key server. This setup removes the need for the vCenter Server and workload ESXi hosts from requiring direct key server credentials, and enables an extra layer of defense-in-depth security.
Trusted Key Provider	A Key Provider that encapsulates a single encryption key on a key server. Access to the encryption key requires the Attestation Service to acknowledge that the ESXi software has been verified on the Trusted Host.
Standard Key Provider	A Key Provider that gets encryption keys directly from a key server, and distributes keys to the required hosts in a data center. Previously referred to in vSphere as KMS Cluster.
Key Server	A KMIP key management server (KMS) that is associated with a Key Provider.
Workload vCenter Server	The vCenter Server that manages and is used to configure one or more Trusted Clusters.

vSphere Trust Authority Basics

With vSphere Trust Authority, you can:

- Provide ESXi hosts with a hardware root of trust and remote attestation capabilities
- Restrict encryption key management by releasing keys only to attested ESXi hosts
- Create a more secure administrative environment for managing trust

- Centralize management of multiple key servers
- Continue to perform cryptographic operations on virtual machines but with an enhanced level of encryption key management

In vSphere 6.5 and 6.7, virtual machine encryption depends on vCenter Server to obtain encryption keys from a key server and push them to ESXi hosts as needed. vCenter Server authenticates with the key server by using client and server certificates, which are stored in VMware Endpoint Certificate Store (VECS). Encryption keys that are sent from the key server pass through vCenter Server memory to the required ESXi hosts (with data encryption provided by TLS over the wire). In addition, vSphere depends on privilege checks in vCenter Server to validate user permissions and enforce key server access restrictions. Although this architecture is secure, it does not address the potential for a compromised vCenter Server, a rogue vCenter Server administrator, or a management or configuration error that might result in leaked or stolen secrets.

In vSphere 7.0, vSphere Trust Authority addresses these problems. You can create a trusted computing base, which consists of a secure, manageable set of ESXi hosts. vSphere Trust Authority implements a remote attestation service for the ESXi hosts you want to trust. Furthermore, vSphere Trust Authority improves upon TPM 2.0 attestation support (added to vSphere beginning in the 6.7 release), to implement access restrictions on encryption keys and so better protect virtual machine workload secrets. In addition, vSphere Trust Authority allows only authorized Trust Authority administrators to configure vSphere Trust Authority services, and configure Trust Authority hosts. The Trust Authority administrator can be the same user as the vSphere administrator user, or a separate user.

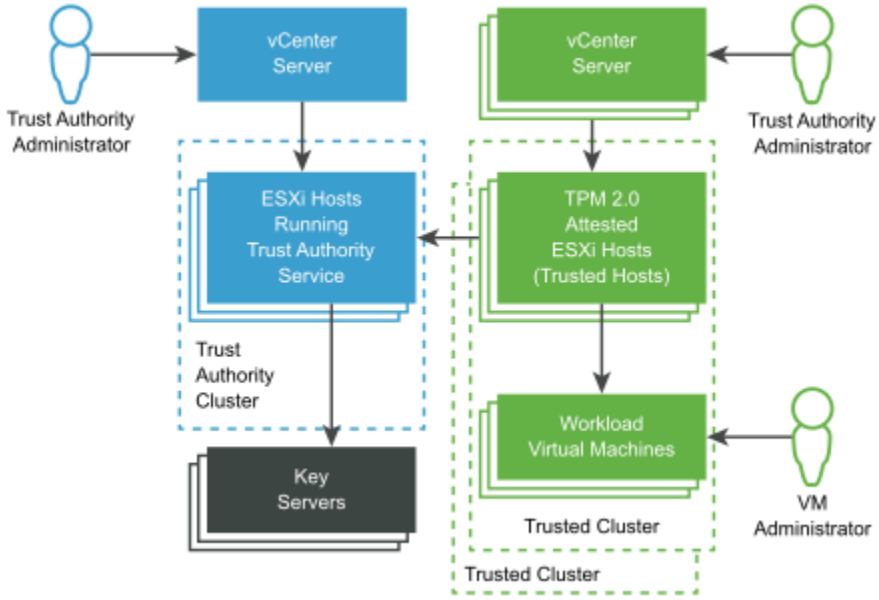
In the end, vSphere Trust Authority enables you to run your workloads in a more safe and secure environment by:

- Detecting tampering
- Disallowing unauthorized changes
- Preventing malware and modifications
- Limiting sensitive workloads to run only on a verified, safe hardware and software stack

vSphere Trust Authority Architecture

The following figure shows a simplified view of the vSphere Trust Authority architecture.

Figure 90: vSphere Trust Authority Architecture



In this figure:

1. vCenter Server systems
   Separate vCenter Server systems manage the Trust Authority Cluster and Trusted Clusters.
2. Trust Authority Cluster
   Consists of the ESXi hosts that run the vSphere Trust Authority components.
3. Key Servers
   Store encryption keys that are used by the Key Provider Service when encryption operations are performed. The key servers are external to vSphere Trust Authority.
4. Trusted Clusters
   Consist of the ESXi Trusted Hosts, which have been remotely attested with a TPM, and that run encrypted workloads.
5. Trust Authority Administrator
   Administrator who is a member of the vCenter Server TrustedAdmins group, and configures the Trusted Infrastructure.
   vSphere Trust Authority enables flexibility in how you designate Trust Authority administrators. The Trust Authority administrators in the figure can be separate users. It is also possible for the Trust Authority administrators to be the same user, using credentials that are linked across the vCenter Server systems. In this case, it is the same user and the same TrustedAdmins group.
6. VM Administrator
   Administrator who has been granted privileges to manage the encrypted workload virtual machines on the Trusted Hosts.

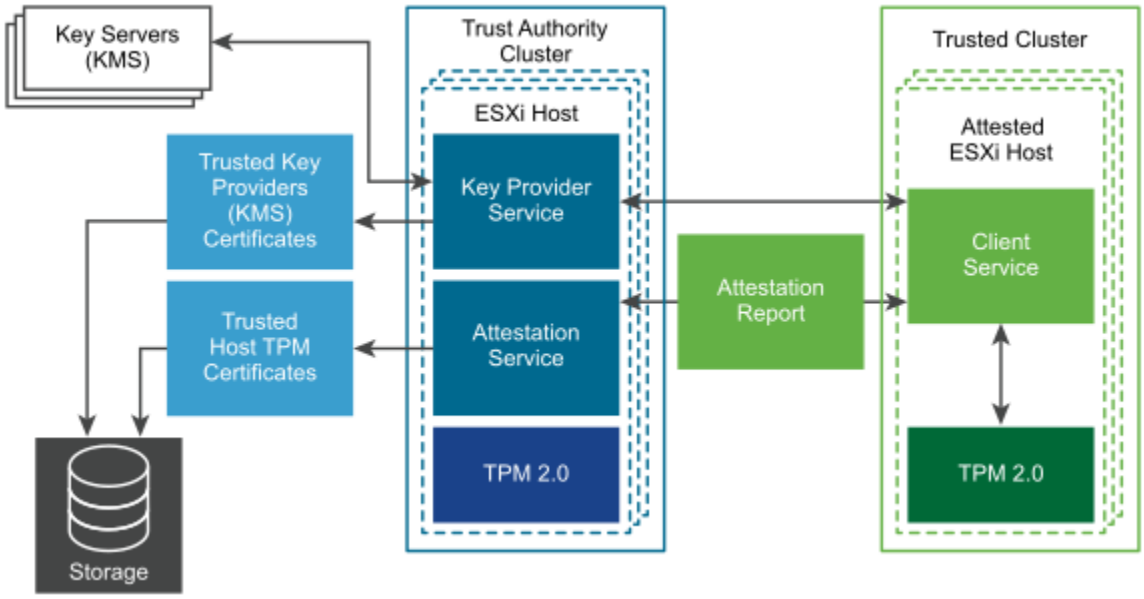
Trusted Infrastructure Overview

vSphere Trust Authority services, at least one external KMIP-compliant key server, the vCenter Server systems, and your ESXi hosts contribute to the Trusted Infrastructure.

What Is a Trusted Infrastructure

A Trusted Infrastructure consists of at least one vSphere Trust Authority Cluster, at least one Trusted Cluster, and at least one external KMIP-compliant key server. Each cluster contains ESXi hosts that run specific vSphere Trust Authority services, as shown in the following figure.

Figure 91: vSphere Trust Authority Services



Configuring the Trust Authority Cluster enables two services:

- Attestation Service
- Key Provider Service

When you configure vSphere Trust Authority, the ESXi hosts in the Trusted Cluster communicate with the Attestation Service. The Key Provider Service interposes between the Trusted Hosts and one or more trusted key providers.

Note: Currently, the ESXi hosts in the Trust Authority Cluster do not require a TPM. However, as a matter of best practice, consider installing new ESXi hosts with TPMs.

About the vSphere Trust Authority Attestation Service

The Attestation Service generates a signed document that contains assertions describing the binary and configuration state of the remote ESXi hosts in the Trusted Cluster. The Attestation Service attests the state of the ESXi hosts using a Trusted Platform Module (TPM) 2.0 chip as its basis for software measurement and reporting. The TPM on the remote ESXi host measures the software stack and sends the configuration data to the Attestation Service. The Attestation Service verifies that the software measurement signature can be attributed to a previously configured trusted TPM endorsement key (EK). The Attestation Service also ensures that the software measurement matches one of a set of previously blessed ESXi images. The Attestation Service signs a JSON Web Token (JWT) that it issues to the ESXi host, providing the assertions about the identity, validity, and configuration of the ESXi host.

What Is the vSphere Trust Authority Key Provider Service

The Key Provider Service removes the need for the vCenter Server and the ESXi hosts from requiring direct key server credentials. In vSphere Trust Authority, for an ESXi host to have access to an encryption key, it must authenticate with the Key Provider Service.

For the Key Provider Service to connect to a key server, the Trust Authority administrator must configure a trust setup. For most KMIP-compliant servers, configuring a trust setup involves configuring client and server certificates.

To ensure that the keys are released only to ESXi Trusted Hosts, the Key Provider Service acts as a gatekeeper to the key servers. The Key Provider Service hides the key server specifics from the rest of the data center software stack by using the concept of a trusted key provider. Each trusted key provider has a single configured primary encryption key, and references one or more key servers. The Key Provider Service can have several configured trusted key providers. For example, you might want to have a separate trusted key provider for each department in an organization. Each trusted key provider uses a different primary key, but can reference the same backing key server.

After you create a trusted key provider, the Key Provider Service can accept requests from the ESXi Trusted Hosts to run cryptographic operations against that trusted key provider.

When an ESXi Trusted Host requests operations against a trusted key provider, the Key Provider Service makes sure that the ESXi host that is trying to obtain the encryption key is attested. After passing all the checks, the ESXi Trusted Host receives encryption keys from the Key Provider Service.

What Ports Are Used by vSphere Trust Authority

The vSphere Trust Authority services listen for connections behind the ESXi host's reverse proxy. All communication occurs over HTTPS on port 443.

What Are vSphere Trust Authority Trusted Hosts

The ESXi Trusted Hosts are configured to use trusted key providers to perform cryptographic operations. The ESXi Trusted Hosts perform key operations by communicating to the Key Provider Service and the Attestation Service. For authentication and authorization, the ESXi Trusted Hosts use a token obtained from the Attestation Service. To get a valid token, the ESXi Trusted Host must successfully attest to the Attestation Service. The token contains certain claims that are used to decide whether the ESXi Trusted Host is authorized to access a trusted key provider.

vSphere Trust Authority and Key Servers

vSphere Trust Authority requires the use of at least one key server. In previous vSphere releases, a key server was called a Key Management Server or KMS. Currently, vSphere virtual machine encryption solution supports KMIP 1.1 compliant key servers.

How Does vSphere Trust Authority Store Configuration and State Information

vCenter Server is mostly a pass-through service for vSphere Trust Authority configuration and state information. Most vSphere Trust Authority configuration and state information is stored on the ESXi hosts in the ConfigStore database. Some state information is stored in the vCenter Server database as well.

Note: Because most vSphere Trust Authority configuration information is stored on the ESXi hosts, the vCenter Server file-based backup mechanism does not back up this information. To ensure the configuration information for your vSphere Trust Authority deployment is saved, see Backing Up the vSphere Trust Authority Configuration.

How Does vSphere Trust Authority Integrate with vCenter Server

You configure separate vCenter Server instances to manage the Trust Authority Cluster and Trusted Cluster. See Configuring vSphere Trust Authority.

On a Trusted Cluster, the vCenter Server manages the Trust Authority API calls and passes them through to the ESXi hosts. The vCenter Server replicates the API calls across all ESXi hosts in the Trusted Cluster.

After you configure vSphere Trust Authority initially, you can add or remove ESXi hosts to or from a Trust Authority Cluster or a Trusted Cluster. See Adding and Removing vSphere Trust Authority Hosts.

vSphere Trust Authority Process Flows

Understanding vSphere Trust Authority process flows is essential to learning how to configure and manage your Trusted Infrastructure.

How Do You Configure vSphere Trust Authority

vSphere Trust Authority is not activated by default. You must manually configure vSphere Trust Authority in your environment. See Configuring vSphere Trust Authority.

When you configure vSphere Trust Authority, you must specify which versions of ESXi software the Attestation Service accepts, and also which Trusted Platform Modules (TPMs) are trustworthy.

TPM and Attestation

This guide uses the following definitions when discussing TPMs and attestation.

Table 257: TPM and Attestation Glossary

Term	Definition
Endorsement Key (EK)	A TPM is manufactured with an RSA public/private key pair built into the hardware, called the endorsement key (EK). The EK is unique to a particular TPM.
EK Public Key	The public portion of the EK key pair.
EK Private Key	The private portion of the EK key pair.

Term	Definition
EK Certificate	The EK public key wrapped with a signature. The EK certificate is created by the TPM manufacturer who uses its Certificate Authority private key to sign the EK public key. Not all TPMs contain an EK certificate. In this case, the EK public key is not signed.
TPM Attestation	The ability of the Attestation Service to verify the software that is running on a remote host. TPM attestation is accomplished through cryptographic measurements made by the TPM while the remote host starts, and is relayed to the Attestation Service on request. The Attestation Service establishes trust in the TPM through either the EK public key or the EK certificate.

Configuring TPM Trust on the Trusted Hosts

An ESXi Trusted Host must contain a TPM. A TPM is manufactured with a public/private key pair built into the hardware, called the endorsement key (EK). Although TPM 2.0 permits many key/certificate pairs, the most common is an RSA-2048 key pair. When a TPM EK public key is signed by a CA, the result is the EK certificate. The TPM manufacturer typically pre-generates at least one EK, signs the public key with a Certificate Authority, and embeds the signed certificate in the TPM's non-volatile memory.

You can configure the Attestation Service to trust TPMs as follows:

- Trust all CA certificates with which the manufacturer signed the TPM (the EK public key). The default setting for the Attestation Service is to trust CA certificates. In this approach, the same CA certificate covers many ESXi hosts, and so reduces your administrative overhead.
- Trust the ESXi host's TPM CA certificate and EK public key. The latter can be either the EK certificate or the EK public key. Although this approach provides more security, it requires you to configure information about each Trusted Host.
- Some TPMs do not contain an EK certificate. In this case, you trust the EK public key.

Deciding to trust all TPM CA certificates is operationally convenient. You configure new certificates only when you add a new class of hardware to your data center. By trusting individual EK certificates, you can limit access to specific ESXi hosts.

You can also decide not to trust TPM CA certificates. Though an uncommon situation, you can use this configuration when an EK is not signed by a CA. Currently, this functionality is not fully implemented.

Note: Some TPMs do not include EK certificates. If you want to trust individual ESXi hosts, the TPM must include an EK certificate.

Attesting TPMs

To begin the attestation process, the ESXi Trusted Host in the Trusted Cluster sends the pre-configured EK public key and EK certificate to the Attestation Service on the Trust Authority Cluster. When the Attestation Service receives the request, it looks up the EK in its configuration, which can be the EK public key or the EK certificate, or both, depending on the configuration. If no case is valid, the Attestation Service rejects the attestation request.

The EK is not directly used for signing, so an Attestation Key (AK or AIK) is negotiated. The negotiation protocol ensures that a newly created AK is bound to the previously verified EK, preventing a man-in-the-middle situation, or an impersonator. After an AK is negotiated, it is reused on future attestation requests rather than generating a new one each time.

The ESXi Trusted Host reads the Quote and PCR values from the TPM. The Quote is signed by the AK. The ESXi Trusted Host also reads the TCG Event Log, which includes all the events that resulted in the current PCR state. This TPM

information is sent to the Attestation Service for validation. The Attestation Service verifies the PCR values using the event log.

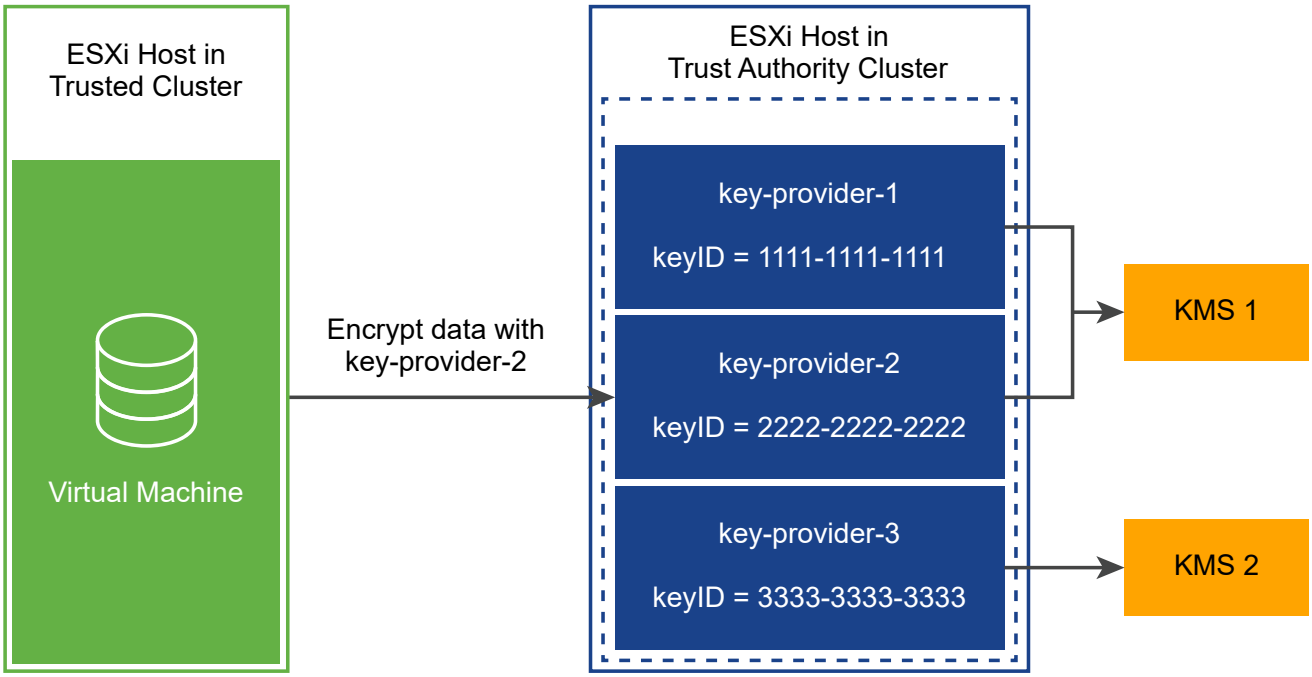
How Do Key Providers Work with Key Servers

The Key Provider Service uses the concept of a trusted key provider to hide the key server specifics from the rest of the data center software. Each trusted key provider has a single configured primary encryption key, and references one or more key servers. The primary encryption key is present in the key servers. As part of configuring vSphere Trust Authority, you must provision the primary key as a separate activity and activate it. The Key Provider Service can have several configured trusted key providers. Each trusted key provider uses a different primary key, but can reference the same backing key server.

When a new trusted key provider is added, the Trust Authority administrator must specify the key server and an existing key identifier on that key server.

The following figure shows the relationship between the Key Provider Service and key servers.

Figure 92: Key Provider and Key Server



After you configure a trusted key provider for a Trusted Cluster, the Key Provider Service can accept requests to run cryptographic operations against that trusted key provider. For example, in this figure, three trusted key providers are configured, two for KMS-1, and one for KMS-2. The Trusted Host requests an encryption operation against key-provider-2. The Trusted Host requests an encryption key to be generated and returned, and uses this encryption key to perform encryption operations.

The Key Provider Service uses the primary key referenced by key-provider-2 to encrypt the specified plaintext data and return the corresponding ciphertext. Later, the Trusted Host can provide the same ciphertext to a decrypt operation and get back the original plaintext.

vSphere Trust Authority Authentication and Authorization

vSphere Trust Authority administrative operations require a user that is a member of the TrustedAdmins group. Having only Trust Authority administrator privileges is not sufficient to perform all administrative operations that involve the ESXi hosts. For more information, see Prerequisites and Required Privileges for vSphere Trust Authority.

Adding a Trusted Host to a Trusted Cluster

The steps to add ESXi hosts initially to the Trusted Cluster are described in Configuring vSphere Trust Authority.

Later, if you want to add ESXi hosts to the Trusted Cluster, the workflow is different. See Adding and Removing vSphere Trust Authority Hosts.

When you initially add ESXi hosts to the Trusted Cluster, you must gather the following information:

- TPM certificate for each type of hardware in the cluster
- ESXi image for each version of ESXi in the cluster
- vCenter Server principal information

If you later add ESXi hosts to a Trusted Cluster, you might need to collect some additional information. That is, if the new ESXi hosts differ in hardware or ESXi version from the original hosts, you must collect the new ESXi host information and import it to the Trust Authority Cluster. You only must collect the vCenter Server principal information one time per vCenter Server system.

vSphere Trust Authority Topology

vSphere Trust Authority requires separate vCenter Server systems for the Trust Authority Cluster and the Trusted Cluster.

The Trust Authority Cluster is configured and managed on an independent, isolated vCenter Server. The vCenter Server of the Trust Authority Cluster cannot also be the vCenter Server of the Trusted Cluster. The Trusted Cluster must have its own, separate vCenter Server. A single vCenter Server can manage multiple Trusted Clusters. Multiple vCenter Server systems for Trusted Clusters can participate in enhanced linked mode. The vCenter Server for the Trust Authority Cluster cannot participate in enhanced linked mode with other Trust Authority Cluster vCenter Server systems or Trusted Cluster vCenter Server systems.

The Trust Authority administrator manages the Trust Authority Cluster and its associated vCenter Server independently from other vCenter Server instances, because this approach provides the best security isolation.

The Trust Authority administrator documents or publishes the hostnames and SSL certificates that Trusted Cluster administrators use to configure their clusters. The Trust Authority administrator also provisions trusted key providers for the organization and its departments, or even individual administrators.

You cannot deploy vSphere Trust Authority services directly on the Trusted Cluster managed by the Workload vCenter Server, because the workload administrator has high privilege access to the ESXi hosts. This type of deployment does not achieve the necessary separation of roles that is required to meet the security objectives of vSphere Trust Authority.

Prerequisites and Required Privileges for vSphere Trust Authority

You must consider hardware and software requirements when configuring vSphere Trust Authority. You must set cryptographic privileges and roles to use encryption. The user who performs vSphere Trust Authority tasks must have the appropriate privileges.

Requirements for vSphere Trust Authority

To use vSphere Trust Authority, your vSphere environment must meet these requirements:

- ESXi Trusted Host hardware requirements:
  - TPM 2.0
  - Secure boot must be enabled
  - EFI firmware
- Component requirements:
  - vCenter Server 7.0 or later
  - A dedicated vCenter Server system for the vSphere Trust Authority Cluster and ESXi hosts
  - A separate vCenter Server system for the Trusted Cluster and ESXi Trusted Hosts
  - A key server (called a Key Management Server, or KMS, in prior vSphere releases)
- Virtual machine requirements:
  - EFI firmware
  - Secure Boot Enabled

Note: Before you can begin configuring vSphere Trust Authority, ensure that you have set up your vCenter Server systems for the Trust Authority Cluster and Trusted Cluster, and added ESXi hosts to each cluster.

Cryptography Privileges

vSphere Trust Authority does not introduce any new cryptography privileges. The same cryptography privileges described in Cryptography Privileges and Roles apply to vSphere Trust Authority.

Host Encryption Mode

vSphere Trust Authority does not introduce any new requirements for enabling host encryption mode on the ESXi Trusted Hosts. See Prerequisites and Required Privileges for Encryption Tasks for more information about host encryption mode.

About the vSphere Trust Authority Roles and the TrustedAdmins Group

vSphere Trust Authority operations require a user that is a member of the TrustedAdmins group. This user is called the Trust Authority administrator. vSphere administrators must either add themselves to the TrustedAdmins group or add other users to the group to gain the Trusted Infrastructure administrator role. The Trusted Infrastructure administrator role is necessary for vCenter Server authorization. The TrustedAdmins group is necessary for authentication on the ESXi hosts that are part of the Trusted Infrastructure. Users with the **Cryptographic Operations** > **Register host** privilege on ESXi hosts can manage the Trusted Cluster. The vCenter Server permissions are not propagated to the Trust Authority hosts, only to the Trusted Hosts. Only members of the TrustedAdmins group are granted privileges on the Trust Authority hosts. Group membership is verified on the ESXi host itself.

Note: vSphere administrators and members of the Administrators group are assigned the Trusted Infrastructure administrator role, but this role by itself does not permit a user to perform vSphere Trust Authority operations. Membership in the TrustedAdmins group is also required.

After vSphere Trust Authority is enabled, Trust Authority administrators can assign trusted key providers to Trusted Hosts. Those Trusted Hosts can then use the trusted key providers to perform cryptographic tasks.

In addition to the Trusted Infrastructure administrator role, vSphere Trust Authority provides the No Trusted Infrastructure administrator role, which contains all privileges in vCenter Server except the ones that call the vSphere Trust Authority APIs.

vSphere Trust Authority groups, roles, and users function as follows:

- On first boot, vSphere grants the TrustedAdmins group the Trusted Infrastructure administrator role, which has global permissions.

- The Trusted Infrastructure administrator role is a system role that has the required privileges to call the vSphere Trust Authority APIs (`TrustedAdmin.*`), and the system privileges **System.Read**, **System.View**, and **System.Anonymous** to view inventory objects.
- The No Trusted Infrastructure administrator role is a system role that contains all privileges in vCenter Server except the ones to call the vSphere Trust Authority APIs. Adding new privileges to vCenter Server also adds them to the No Trusted Infrastructure administrator role. (The No Trusted Infrastructure administrator role is similar to the No cryptography administrator role.)
- The vSphere Trust Authority privileges (`TrustedAdmin.*` APIs) are not included in the No cryptography administrator role, preventing users with this role from setting up a Trusted Infrastructure or performing cryptographic operations.

The use cases for these users, groups, and roles, are shown in the following table.

Table 258: vSphere Trust Authority Users, Groups, and Roles

User, Group, or Role	Can Call vSphere Trust AuthorityvCenter Server API (Includes Calls to vSphere Trust AuthorityESXi API)	Can Call vSphere Trust AuthorityvCenter Server API (Does Not Include Calls to vSphere Trust AuthorityESXi API)	Can Perform Host Operations in Cluster Not Related to vSphere Trust Authority	Comment
User in both Administrators@*system.domain* group and TrustedAdmins@*system.domain* group	Yes	Yes	Yes	NA
User in TrustedAdmins@*system.domain* group only	Yes	Yes	No	Such a user cannot perform regular cluster management operations.
User in Administrators@*system.domain* group only	Yes	No	Yes	NA
User with Trusted Infrastructure administrator role but not in TrustedAdmins@*system.domain* group	Yes	No	No	The ESXi host checks the group membership of the user to grant permissions.
User with No Trusted Infrastructure administrator role only	No	No	Yes	Such a user is similar to an administrator who cannot perform vSphere Trust Authority operations.

vSphere Trust Authority Best Practices, Caveats, and Interoperability

The vSphere Trust Authority architecture results in some additional recommendations. As you are planning your vSphere Trust Authority strategy, consider interoperability limitations.

Trusted Infrastructure Interoperability

For ESXi versions, the Attestation Service is backward and forward compatible. For example, you can have a cluster of ESXi hosts running ESXi 7.0 in the vSphere Trust Authority Cluster, and upgrade or patch ESXi hosts in the Trusted

Cluster to a newer ESXi version. Similarly, you can upgrade or patch the ESXi hosts in the Trust Authority Cluster while keeping the ESXi hosts in the Trusted Cluster at the current version.

You cannot have a cluster function as both a Trust Authority Cluster and a Trusted Cluster. This configuration is not supported.

Trusted Cluster Configuration Limitation

You can configure only one Trusted Cluster per workload vCenter Server. A Trusted Cluster cannot be configured to reference multiple Trust Authority Clusters.

Supported Features

vSphere Trust Authority supports the following:

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM, with the following understanding:
  - SRM with array-based replication is supported, if the same vSphere Trust Authority services configuration is available on the recovery side.
  - SPPG
- VADP
  - Support is the same as with standard encryption. Hot-add and NFC modes are supported, but not SAN mode. Backups are decrypted. VADP partners have the option of recovering the backed-up virtual machine with the same encryption key as the original virtual machine.
- vSAN
  - Virtual machine encryption is fully supported on top of vSAN.
- OVF
  - Encrypted virtual machines cannot be exported to OVF. However, virtual machines can be encrypted while being imported from an OVF.
- VVol

Unsupported Features

Currently, vSphere Trust Authority does not support the following:

- vSAN encryption
- First Class Disk (FCD) encryption
- vSphere Replication
- vSphere Host Profiles

vSphere Trust Authority Life Cycle

The vSphere Trust Authority services are packaged and installed as part of the base ESXi image.

Starting and Stopping Services

In the vSphere Client, you can start, stop, and restart vSphere Trust Authority services that are running on an ESXi host. You can restart services upon a configuration change or if you suspect functional or performance problems. To restart the service on an ESXi Trusted Host, you must log in to the host itself to restart the service. See Start, Stop, and Restart vSphere Trust Authority Services.

Upgrading and Patching

Each time you upgrade or patch an ESXi Trusted Host, you must update the vSphere Trust Authority Cluster with the new ESXi version information. One way to do so is to upgrade or patch a test ESXi host, export the ESXi base image information, import the image file to the Trust Authority Cluster, then upgrade or patch the ESXi Trusted Hosts.

Upgrading Best Practices

Best practice for upgrading a vSphere Trust Authority infrastructure is to upgrade the Trust Authority vCenter Server and Trust Authority Hosts first. In this way, you get the most benefit from the latest vSphere Trust Authority features. However, you can perform separate, standalone upgrades of vCenter Server and ESXi hosts to fit specific business reasons.

In general, follow this order for upgrading your vSphere Trust Authority infrastructure:

1. Upgrade the Trust Authority Cluster vCenter Server.
2. Upgrade the Trust Authority Hosts.
3. Upgrade the Trusted Cluster vCenter Server.
4. Upgrade the Trusted Hosts.

To ensure a smooth process, upgrade your Trust Authority Hosts and Trusted Hosts gradually, one-by-one.

Troubleshooting Upgrade Problems

If you encounter an unsuccessful upgrade of a Trust Authority Host, follow these steps.

1. Remove the Trust Authority Host from the Trusted Cluster.
2. Revert to the previous version of ESXi.
3. Re-add the Trust Authority Host to the cluster as described in the VMware knowledge base article at https://kb.vmware.com/s/article/77234.
4. Verify that the Trust Authority Host's configuration is consistent with the other Trust Authority Hosts in the Trust Authority Cluster. See Check Trusted Cluster Health.

When you upgrade to a new version of ESXi on a Trusted Host, attestation fails until you update the Trust Authority Cluster with the new ESXi base image information. This behavior is to be expected. You can no longer encrypt virtual machines or use existing virtual machines that were encrypted before upgrade until you fix the problem. Attestation error messages appear in the vSphere Client **Recent Tasks** pane and the `attestd.log`, `kmxa.log`, and `vpxd.log` files.

To correct the problem, follow these steps.

1. Run the `Export-VMHostImageDb` cmdlet to re-export the ESXi base images. See Step 5 in Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
2. Run the `New-TrustAuthorityVMHostBaseImage` cmdlet to reimport the new base image to the vCenter Server of the Trust Authority Cluster. See Step 8 in Import the Trusted Host Information to the Trust Authority Cluster.
3. If you no longer must attest the older versions of ESXi (all the Trusted Hosts have been upgraded), run the `Remove-TrustAuthorityVMHostBaseImage` cmdlet to remove the versions. For example:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

Backing Up the vSphere Trust Authority Configuration

Because most vSphere Trust Authority configuration information is stored on the ESXi hosts, the vCenter Server Backup does not back up this vSphere Trust Authority information. See Backing Up the vSphere Trust Authority Configuration.

Configuring vSphere Trust Authority

vSphere Trust Authority is not enabled by default. You must configure your environment for vSphere Trust Authority before you can start using it.

You enable vSphere Trust Authority services on a dedicated vCenter Server cluster, known as the vSphere Trust Authority Cluster. The Trust Authority Cluster acts as a centralized, secure management platform. You then enable a workload vCenter Server cluster as the Trusted Cluster. The Trusted Cluster contains the ESXi Trusted Hosts.

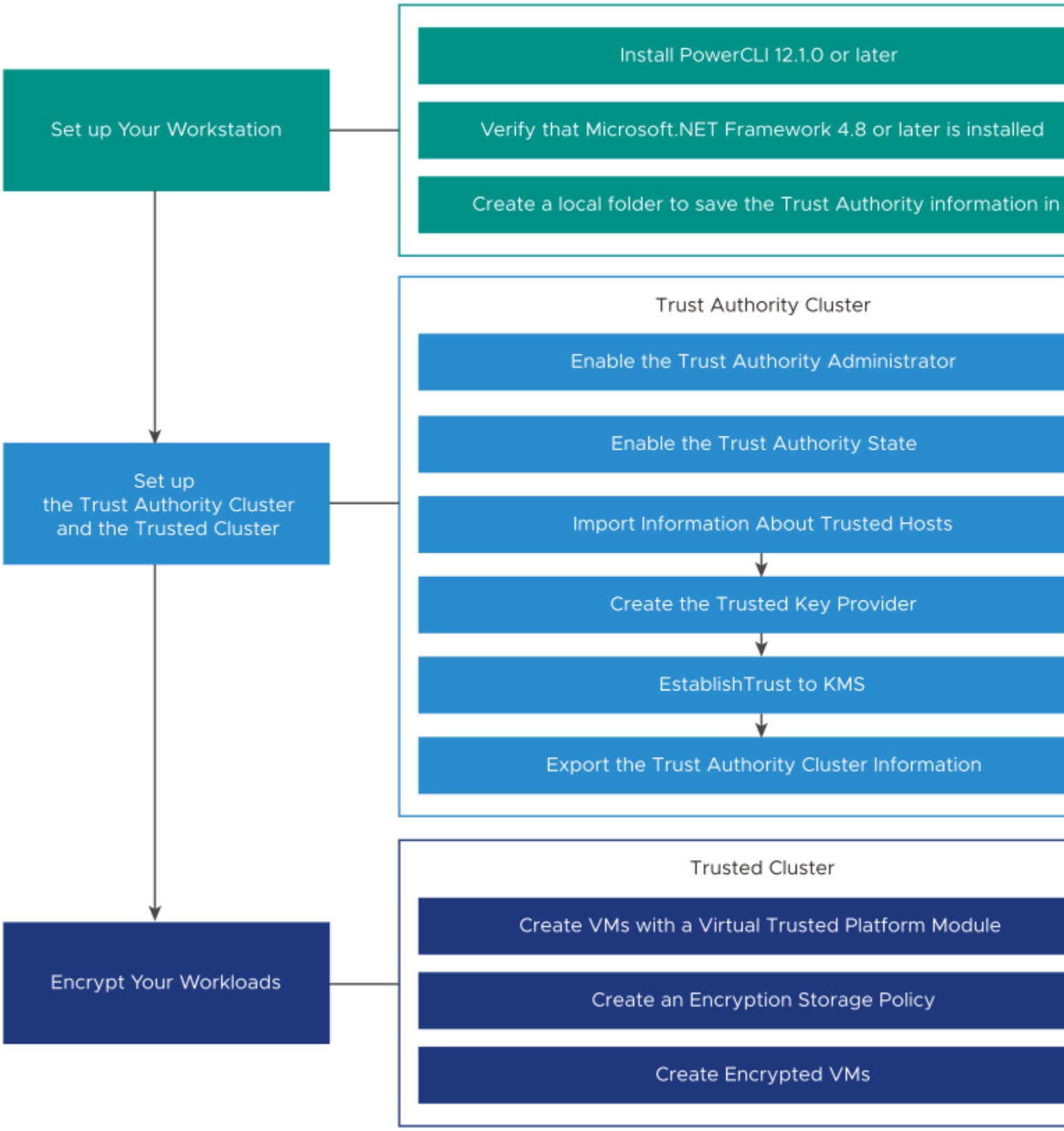
The Trust Authority Cluster attests the ESXi hosts in the Trusted Cluster remotely. The Trust Authority Cluster releases encryption keys only to attested ESXi hosts in the Trusted Cluster to encrypt virtual machines and virtual disks using trusted key providers.

Before you begin configuring vSphere Trust Authority, see Prerequisites and Required Privileges for vSphere Trust Authority for information on the required setup of vCenter Server systems and ESXi hosts.

You manage different aspects of vSphere Trust Authority in the following ways.

- Configure the vSphere Trust Authority services and trusted connections using PowerCLI cmdlets or the vSphere APIs. See *VMware PowerCLI Cmdlets Reference* and *vSphere Automation SDKs Programming Guide*.
- Manage the configuration of trusted key providers using the PowerCLI cmdlets or from the vSphere Client.
- Perform encryption workflows, as in prior vSphere releases, using the vSphere Client and APIs.

Figure 93: vSphere Trust Authority Workflow



To configure and manage vSphere Trust Authority, you use VMware PowerCLI, though some functionality is available in the vSphere Client.

When you configure vSphere Trust Authority, you must complete setup tasks on both the Trust Authority Cluster and the Trusted Cluster. Some of these tasks are order-specific. Use the task sequence outlined in this guide.

Note: When adding more ESXi hosts to the Trusted Cluster after completing the initial vSphere Trust Authority setup, you might need to export and import the Trusted Host information again. That is, if the new ESXi hosts differ from the original hosts, you must collect the new ESXi host information and import it to the Trust Authority Cluster. See Adding and Removing vSphere Trust Authority Hosts.

Set up Your Workstation

To configure a vSphere Trust Authority deployment, you must first prepare a workstation with the necessary software and setup.

Perform the following steps on a workstation that has access to your vSphere Trust Authority environment.

1. Install PowerCLI 12.1.0 or later. See *PowerCLI User's Guide*.
2. Verify that Microsoft .NET Framework 4.8 or later is installed.
3. Create a local folder in which to save the Trust Authority information that you export as files.

Continue with Enable the Trust Authority Administrator.

Enable the Trust Authority Administrator

To enable vSphere Trust Authority, you must add a user to the vSphere TrustedAdmins group. This user becomes the Trust Authority administrator. You use the Trust Authority administrator for most vSphere Trust Authority configuration tasks.

Either create or a user, or identify an existing user, to be the Trust Authority administrator.

Use a separate user from the vCenter Server administrator as your Trust Authority administrator. Having a separate user enhances the security of your environment. You must enable a Trust Authority administrator for both the Trust Authority Cluster and the Trusted Cluster.

1. Connect to the vCenter Server of the Trust Authority Cluster by using the vSphere Client.
2. Log in as an administrator.
3. From the **Home** menu, select **Administration**.
4. Under **Single Sign On**, click **Users and Groups**.
5. Click **Groups** and click the **TrustedAdmins** group.

   If the TrustedAdmins group does not appear initially, use the **Filter** icon to filter for it, or navigate through the groups by clicking the right arrow at the bottom of the pane.
6. In the **Group Members** area, click **Add Members**.

   Make sure that the local identity source is selected (vsphere.local is the default, but you might have selected a different domain during installation), and search for the member (user) you want to add to the group as the Trust Authority administrator.
7. Select the member.
8. Click **Save**.
9. Repeat steps 1 through 8 for the vCenter Server of the Trusted Cluster.

Continue with Enable the Trust Authority State.

Enable the Trust Authority State

Making a vCenter Server cluster into a vSphere Trust Authority Cluster (also called enabling the Trust Authority State) starts the required Trust Authority services on the ESXi hosts in the cluster.

- Enable the Trust Authority Administrator.

1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as the Trust Authority administrator user to the vCenter Server of the Trust Authority Cluster.

   ```
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

2. To check the current state of the cluster, run the `Get-TrustAuthorityCluster` cmdlet.
   For example, this command shows the cluster, `vTA Cluster` , and that its state is disabled.

   ```
   Get-TrustAuthorityCluster

   Name                 State                Id
   ----                 -----                --
   vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8
   ```

   The output shows either Disabled or Enabled in the State column for each cluster found. Disabled means that the Trust Authority services are not running.

3. To enable the Trust Authority Cluster, run the `Set-TrustAuthorityCluster` cmdlet.
   For example, this command enables the cluster `vTA Cluster` .

   ```
   Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
   ```

   The system responds with a confirmation prompt.

   ```
   Confirmation
   Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
   [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
   ```

4. At the confirmation prompt, press Enter. (The default is `Y`.)

   The output shows the state of the cluster. For example, the following shows that cluster `vTA Cluster` has been enabled:

   ```
   Name                 State                Id
   ----                 -----                --
   vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
   ```

Two services start on the ESXi hosts in the Trust Authority Cluster: the Attestation Service and the Key Provider Service.

Enable the Trusted State on the Trust Authority Cluster

This example shows how to use PowerCLI to enable services on the Trust Authority Cluster. The following table shows the example components and values that are used.

Table 259: Example vSphere Trust Authority Setup

Component	Value
vCenter Server for Trust Authority Cluster	192.168.210.22
Trust Authority Cluster name	vTA Cluster
Trust Authority administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User trustedadmin@v-
sphere.local -Password 'VMware1!'
```

```
Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -
State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

Continue with Collect Information About ESXi Hosts and vCenter Server to Be Trusted.

Collect Information About ESXi Hosts and vCenter Server to Be Trusted

To establish trust, the vSphere Trust Authority Cluster requires information about the Trusted Cluster's ESXi hosts and vCenter Server. You export this information as files for importing into the Trust Authority Cluster. You must ensure to keep these files confidential and transport them securely.

- Identify the ESXi versions and TPM hardware types that are in the Trusted Cluster, and whether you want to trust all TPM hardware types, only certain ones, or individual hosts.
- On the machine from which you run the PowerCLI cmdlets, create a local folder in which to save the information you export as files.
- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.

You use vSphere Trust Authority PowerCLI cmdlets to export the following information as files from the ESXi hosts in the Trusted Cluster for the Trust Authority Cluster to know what software and hardware to trust.

- ESXi version
- TPM manufacturer (CA certificate)
- (Optional) Individual TPM (EK certificate)

Note: Store these exported files in a secure location, in case you must restore the vSphere Trust Authority configuration.

If you have hosts of the same type and vendor, and manufactured during the same timeframe and location, you might be able to trust all TPMs by obtaining the CA certificate of only one of the TPMs. To trust an individual TPM, you obtain the EK certificate of the TPM.

You must also obtain the principal information from the Trusted Cluster's vCenter Server. The principal information contains the vpxd solution user and its certificate chain. The principal information enables the Trusted Cluster's vCenter Server to discover the available trusted key providers configured on the Trust Authority Cluster.

To configure vSphere Trust Authority initially, you must collect the ESXi version and TPM information. Also, you must collect the ESXi version each time after you deploy a new version of ESXi, including when you upgrade or apply a patch.

You collect the vCenter Server principal information only one time per vCenter Server system.

1. In a PowerCLI session, run the following commands to disconnect any current connection and connect as the root user to one of the ESXi hosts in the Trusted Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server host_ip_address -User root -Password 'password'
   ```

2. Run the `Get-VMHost` cmdlet to confirm the ESXi host.

   ```
   Get-VMHost
   ```

   The host information is displayed.

3. Assign `Get-VMHost` to a variable.
   For example:

   ```
   $vmhost = Get-VMHost
   ```

4. Run the `Export-Tpm2CACertificate` cmdlet to export the CA certificate of a given TPM manufacturer.
   a) Assign `Get-Tpm2EndorsementKey -VMHost $vmhost` to a variable.
   For example, this command assigns `Get-Tpm2EndorsementKey -VMHost $vmhost` to the variable `$tpm2` .

   ```
   $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
   ```

   b) Run the `Export-Tpm2CACertificate` cmdlet.
   For example, this command exports the TPM certificate to the `cacert.zip` file. Ensure that the destination directory exists before running this command.

   ```
   Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
   ```

   The file is created.
   c) Repeat for each TPM hardware type in the cluster that you want to trust. Use a different file name for each TMP hardware type so that you do not overwrite a previously exported file.

5. Run the `Export-VMHostImageDb` cmdlet to export the ESXi host description of software (the ESXi image).
   For example, this command exports the information to the `image.tgz` file. Ensure that the destination directory exists before running this command.

   ```
   Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
   ```

   Note: The `Export-VMHostImageDb` cmdlet also works if you prefer to log in to the vCenter Server of the Trusted Cluster.

   The file is created.

   Repeat for each ESXi version in the cluster that you want to trust. Use a different file name for each version so that you do not overwrite a previously exported file.

6. Export the Trusted Cluster's vCenter Server principal information.
   a) Disconnect from the ESXi host.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

   b) Connect to the vCenter Server of the Trusted Cluster using the Trust Authority administrator user. (Alternatively, you can use a user that has **Administrator** privileges.)

   ```
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

   c) To export the Trusted Cluster's vCenter Server principal information, run the `Export-TrustedPrincipal` cmdlet.
   For example, this command exports the information to the `principal.json` file. Ensure that the destination directory exists before running this command.

   ```
   Export-TrustedPrincipal -FilePath C:\vta\principal.json
   ```

   The file is created.

7. Optional: If you want to trust an individual host, you must export the TPM EK public key certificate.
   See Export and Import a TPM Endorsement Key Certificate.

The following files are created:

- TPM CA certificate file (.zip file extension)
- ESXi image file (.tgz file extension)
- vCenter Server principal file (.json file extension)

Collecting Information About ESXi Hosts and vCenter Server to Be Trusted

This example shows how to use PowerCLI to export the ESXi host information and the vCenter Server Principal. The following table shows the example components and values that are used.

Table 260: Example vSphere Trust Authority Setup

Component	Value
ESXi host in Trusted Cluster	192.168.110.51
vCenter Server for Trusted Cluster	192.168.110.22
Variable `$vmhost`	`Get-VMHost`
Variable `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`
Trust Authority administrator	trustedadmin@vsphere.local
Local directory to contain output files	`C:\vta`

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB Memory-
TotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
 ------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576         1.614
 7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz

Mode                 LastWriteTime         Length Name
```

```
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM           2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User trustedadmin@v-
sphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

Continue with Import the Trusted Host Information to the Trust Authority Cluster.

Export and Import a TPM Endorsement Key Certificate

You can export a TPM endorsement key (EK) certificate from an ESXi host, and import it to the vSphere Trust Authority Cluster. You do so when you want to trust an individual ESXi host in the Trusted Cluster.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.

To import a TPM EK certificate into the Trust Authority Cluster, you must change the Trust Authority Cluster's default attestation type to accept EK certificates. The default attestation type accepts TPM Certificate Authority (CA) certificates. Some TPMs do not include EK certificates. If you want to trust individual ESXi hosts, the TPM must include an EK certificate.

Note: Store the exported EK certificate files in a secure location, in case you must restore the vSphere Trust Authority configuration.

1. Ensure that you are connected as the Trust Authority administrator to the vCenter Server of the Trust Authority Cluster.
   For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

3. To change the Trust Authority Cluster's attestation type:
   a) Run the `Get-TrustAuthorityCluster` cmdlet to show the clusters managed by this vCenter Server.

      ```
      Get-TrustAuthorityCluster
      ```

The clusters are displayed.

b) Assign the `Get-TrustAuthorityCluster` information to a variable.
For example, this command assigns the cluster named `vTA Cluster` to the variable `$vTA`.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

c) Assign the `Get-TrustAuthorityTpm2AttestationSettings` information to a variable.
For example, this command assigns the information to the variable `$tpm2Settings`.

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

d) Run the `Set-TrustAuthorityTpm2AttestationSettings` cmdlet, specifying `RequireEndorsementKey`, or `RequireCertificateValidation`, or both.
For example, this command specifies `RequireEndorsementKey`.

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings -RequireEndorsementKey
```

The system responds with a confirmation prompt similar to the following.

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with the fol-
lowing parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e) At the confirmation prompt, press Enter. (The default is `Y`.)

The output shows a status of True for the setting specified. For example, this status shows True for Require Endorsement Key, and False for Require Certificate Validation.

```
Name                                 RequireEndorsementKey          RequireCertificateValidation
 Health
----                                 ---------------------          ----------------------------
 ------
TrustAuthorityTpm2AttestationSettings... True                       False
 Ok
```

4. To export the TPM EK certificate:

a) Disconnect from the vCenter Server of the Trust Authority Cluster.

```
Disconnect-VIServer -server * -Confirm:$false
```

b) Run the `Connect-VIServer` cmdlet to connect as the root user to one of the ESXi hosts in the Trusted Cluster.

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c) Run the `Get-VMHost` cmdlet to confirm the ESXi host.

```
Get-VMHost
```

The host information is displayed.

d) Assign `Get-VMHost` to a variable.
For example:

```
$vmhost = Get-VMHost
```

e) Run the `Export-Tpm2EndorsementKey` cmdlet to export the EK certificate of the ESXi host.
For example, this command exports the EK certificate to the `tpm2ek.json` file.

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

The file is created.

5. To import the TPM EK:
   a) Disconnect from the ESXi host in the Trusted Cluster.
      ```
      Disconnect-VIServer -server * -Confirm:$false
      ```
   b) Connect to the vCenter Server of the Trust Authority Cluster using the Trust Authority administrator user.
      ```
      Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
      ```
   c) Run the `Get-TrustAuthorityCluster` cmdlet.
      ```
      Get-TrustAuthorityCluster
      ```
      The clusters in the Trust Authority Cluster are displayed.
   d) Assign the `Get-TrustAuthorityCluster` '*cluster*' information to a variable.
      For example, this command assigns the information for cluster `vTA Cluster` to the variable `$vTA` .
      ```
      $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
      ```
   e) Run the `New-TrustAuthorityTpm2EndorsementKey` cmdlet.
      For example, this command uses the `tpm2ek.json` file previously exported in Step 4.
      ```
      New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath C:\vta\tpm2ek.json
      ```
      The imported endorsement key information is displayed.

The Trust Authority Cluster's attestation type is changed to accept EK certificates. The EK certificate is exported from the Trusted Cluster and imported to the Trust Authority Cluster.

Export and Import a TPM EK Certificate

This example shows how to use PowerCLI to change the Trust Authority Cluster's default attestation type to accept EK certificates, export the TPM EK certificate from the ESXi host in the Trusted Cluster, and import it to the Trust Authority Cluster. The following table shows the example components and values that are used.

Table 261: Example vSphere Trust Authority Setup

Component	Value
vCenter Server for Trust Authority Cluster	192.168.210.22
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
Variable `$vmhost`	`Get-VMHost`
ESXi host in Trusted Cluster	192.168.110.51
Trust Authority administrator	trustedadmin@vsphere.local
Local directory to contain output file	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User trustedadmin@vsphere.local
 -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
```

```
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthori-
tyCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tp-
m2Settings -RequireEndorsementKey

Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with the
 following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                   RequireEndorsementKey          RequireCertificateValida-
tion   Health
----                                   ---------------------
 ----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True                         False
     Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz   MemoryUsageGB
 MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------   -------------
 ------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576           1.230
      7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User trustedadmin@vsphere.local
 -Password 'VMware1!'

Name                           Port  User
```

```
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -
FilePath C:\vta\tpm2ek.json

TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         1a520e42-4db8-1cbb-6dd7-f493fd921ccb    Ok
```

Continue with Import the Trusted Host Information to the Trust Authority Cluster.

Import the Trusted Host Information to the Trust Authority Cluster

You import the exported ESXi host and vCenter Server information into the vSphere Trust Authority Cluster, so that the Trust Authority Cluster knows which hosts it can attest.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.

If you are following these tasks in order, you are still connected to the vCenter Server of the Trust Authority Cluster.

1. Ensure that you are connected as the Trust Authority administrator to the vCenter Server of the Trust Authority Cluster.
   For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.
   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```
3. To show the clusters managed by this vCenter Server, run the `Get-TrustAuthorityCluster` cmdlet.
   ```
   Get-TrustAuthorityCluster
   ```
   The clusters are displayed.
4. Assign the `Get-TrustAuthorityCluster` '*cluster*' information to a variable.
   For example, this command assigns the information for cluster `vTA Cluster` to the variable `$vTA` .
   ```
   $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
   ```
5. To import the vCenter Server principal information of the Trusted Cluster into the Trust Authority Cluster, run the `New-TrustAuthorityPrincipal` cmdlet.
   For example, the following command imports the `principal.json` file previously exported in Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
   ```
   New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
   ```
   The TrustAuthorityPrincipal information is displayed.

6. To verify the import, run the `Get-TrustAuthorityPrincipal` cmdlet.
   For example:
   ```
   Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
   ```
   The imported TrustAuthorityPrincipal information is displayed.
7. To import the Trusted Platform Module (TPM) CA certificate information, run the `New-TrustAuthorityTpm2CACertificate` cmdlet.
   For example, the following command imports the TPM CA certificate information from the `cacert.zip` file previously exported in Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
   ```
   New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath C:\vta\cacert.zip
   ```
   The imported certificate information is displayed.
8. To import the ESXi host base image information, run the `New-TrustAuthorityVMHostBaseImage` cmdlet.
   For example, the following command imports the image information from the `image.tgz` file previously exported in Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
   ```
   New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
   ```
   The imported image information is displayed.

The Trust Authority Cluster knows which ESXi hosts it can remotely attest, and so, which hosts it can trust.

Import the Trusted Host Information to the Trust Authority Cluster

This example shows how to use PowerCLI to import the vCenter Server principal information of the Trusted Cluster and the Trusted Host information files to the Trust Authority Cluster. It assumes that you are connected to the vCenter Server of the Trust Authority Cluster as the Trust Authority administrator. The following table shows the example components and values that are used.

Table 262: Example vSphere Trust Authority Setup

Component	Value
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
vCenter Server for Trust Authority Cluster	192.168.210.22
Trust Authority Cluster names	vTA Cluster1 (Enabled) vTA Cluster2 (Disabled)
Principal information file	`C:\vta\principal.json`
TPM certificate file	`C:\vta\cacert.cer`
ESXi host base image file	`C:\vta\image.tgz`
Trust Authority administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User trustedadmin@vsphere.local
 -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
```

```
----                 -----                --
vTA Cluster1         Enabled              TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled             TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath
 C:\vta\principal.json

Name                                         Domain          Type       TrustAuthorityClusterId
----                                         ------          ----       -----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER   TrustAuthorityCluster-do-
main-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                         Domain          Type       TrustAuthorityClusterId
----                                         ------          ----       -----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER   TrustAuthorityCluster-do-
main-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -
FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -
FilePath C:\vta\image.tgz

TrustAuthorityClusterId                 VMHostVersion                           Health
-----------------------                 -------------                           ------
TrustAuthorityCluster-domain-c8         ESXi 7.0.0-0.0.14828939                 Ok
```

Continue with Create the Key Provider on the Trust Authority Cluster.

Create the Key Provider on the Trust Authority Cluster

For the Key Provider Service to connect to a key provider, you must create a trusted key provider then configure a trust setup between the vSphere Trust Authority Cluster and the key server (KMS). For most KMIP-compliant key servers, this configuration involves setting up client and server certificates.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create and activate a key on the key server to be the primary key for the trusted key provider. This key wraps other keys and secrets used by this trusted key provider. See your key server vendor documentation for more information about creating keys.

What was previously called a KMS Cluster in vSphere 6.7 is now called a key provider in vSphere 7.0. For more information about key providers, see What Is the vSphere Trust Authority Key Provider Service.

In a production environment, you can create multiple key providers. By creating multiple key providers, you can address how to manage your deployment based on company organization, different business units or customers, and so on.

If you are following these tasks in order, you are still connected to the vCenter Server of the vSphere Trust Authority Cluster.

1. Ensure that you are connected to the vCenter Server of the Trust Authority Cluster. For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

3. To create the trusted key provider, run the `New-TrustAuthorityKeyProvider` cmdlet.
   For example, this command uses `1` for the PrimaryKeyID and the name `clkp` . If you are following these tasks in order, you previously assigned `Get-TrustAuthorityCluster` information to a variable (for example, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp -KmipServerAddress ip_address
   ```

   The PrimaryKeyID is normally a key ID that comes from the key server in the form of a UUID. Do not use the key name for PrimaryKeyID. The PrimaryKeyID value is vendor-dependent. See your key server documentation. The `New-TrustAuthorityKeyProvider` cmdlet can take other options, such as `KmipServerPort` , `ProxyAddress` , and `ProxyPort` . See the `New-TrustAuthorityKeyProvider` Help system for more information.

   Each logical key provider, regardless of its type (Standard, Trusted, and Native Key Provider), must have a unique name across all vCenter Server systems.

   For more information, see Key Provider Naming.

   Note: To add multiple key servers to the key provider, use the `Add-TrustAuthorityKeyProviderServer` cmdlet.

   The key provider information is displayed.
4. Establish the trusted connection so that the key server trusts the trusted key provider. The exact process depends on the certificates that the key server accepts, and on your company policy. Select the option appropriate for your server and finish the steps.

Option	See
Upload Client Certificate	Upload the Client Certificate to Establish a Trusted Key Provider Trusted Connection.
Upload KMS certificate and private key	Upload the Certificate and Private Key to Establish a Trusted Key Provider Trusted Connection.
New Certificate Signing Request	Create a Certificate Signing Request to Establish a Trusted Key Provider Trusted Connection.

5. Finish the trust setup by uploading a key server certificate so that the trusted key provider trusts the key server.
   a) Assign the `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` information to a variable.
   For example:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   This variable obtains the trusted key providers in the given Trust Authority Cluster, in this case, `$vTA` .

   Note: If you have more than one trusted key provider, use commands similar to the following to select the one you want:

   ```
   Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   <The trusted key providers listing is displayed.>
   ```

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Using `Select-Object -Last 1` selects the last trusted key provider in the list.

b) To get the key server server certificate, run the `Get-TrustAuthorityKeyProviderServerCertificate` command. For example:

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers
```

The server certificate information is displayed. Initially, the certificate is not trusted, so the Trusted state is False. If you have more than one key server configured, a list of certificates is returned. Verify and add each certificate using the following instructions.

c) Before trusting the certificate, assign `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` information to a variable (for example, `cert`), and run the `$cert.Certificate.ToString()` command and verify the output.
For example:

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers
$cert.Certificate.ToString()
```

The certificate information is displayed, including Subject, Issuer, and other information.

d) To add the KMIP server certificate to the trusted key provider, run `Add-TrustAuthorityKeyProviderServerCertificate`.

For example:

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

The certificate information is displayed and the Trusted state is now True.

6. Verify the status of the key provider.

a) To refresh the key provider status, reassign the `$kp` variable.
For example:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Note: If you have more than one trusted key provider, use commands similar to the following to select the one you want:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Using `Select-Object -Last 1` selects the last trusted key provider in the list.

b) Run the `$kp.Status` command to get the key provider status.
For example:

```
$kp.Status
```

Note: The status can take a few minutes to be refreshed. To view the status, reassign the `$kp` variable and rerun the `$kp.Status` command.

A Health status of Ok indicates that the key provider is running correctly.

The trusted key provider is created and has established trust with the key server.

Create the Key Provider on the Trust Authority Cluster

This example shows how to use PowerCLI to create the trusted key provider on the Trust Authority Cluster. It assumes that you are connected to the vCenter Server of the Trust Authority Cluster as the Trust Authority administrator. It also uses a certificate signed by the key server vendor after submitting a CSR to the vendor.

The following table shows the example components and values that are used.

Table 263: Example vSphere Trust Authority Setup

Component	Value
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
Variable `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
vCenter Server for Trust Authority Cluster	192.168.210.22
KMIP-compliant key server	192.168.110.91
KMIP-compliant key server user	vcqekmip
Trust Authority Cluster name	vTA Cluster
Trust Authority administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User trustedadmin@v-
sphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -Prima-
ryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
 -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
 $kp.KeyProviderServers

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California, C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00CEF192BBF9D80C9F

[Not Before]
```

```
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate -
KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate
 $cert

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

Continue with Export the Trust Authority Cluster Information.

Upload the Client Certificate to Establish a Trusted Key Provider Trusted Connection

Some key server (KMS) vendors require that you upload the trusted key provider's client certificate to the key server. After the upload, the key server accepts traffic that comes from the trusted key provider.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.

1. Ensure that you are connected to the vCenter Server of the Trust Authority Cluster. For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
```

3. Assign the `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` information to a variable. For example:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   If you are following these tasks in order, you previously assigned `Get-TrustAuthorityCluster` information to a variable (for example, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   This variable obtains the trusted key providers in the given Trust Authority Cluster, in this case, `$vTA` .

   Note: If you have more than one trusted key provider, use commands similar to the following to select the one you want:

   ```
   Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   <The trusted key providers listing is displayed.>
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
   ```

   Using `Select-Object -Last 1` selects the last trusted key provider in the list.

4. To create the trusted key provider client certificate, run the `New-TrustAuthorityKeyProviderClientCertificate` cmdlet.
   For example:

   ```
   New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
   ```

   The thumbprint is displayed.

5. To export the key provider client certificate, run the `Export-TrustAuthorityKeyProviderClientCertificate` cmdlet.

   For example:

   ```
   Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
   ```

   The certificate is exported to a file.

6. Upload the certificate file to the key server.

   See your key server documentation for more information.

The trusted key provider has established trust with the key server.

Upload the Certificate and Private Key to Establish a Trusted Key Provider Trusted Connection

Some key server (KMS) vendors require that you configure the trusted key provider with the client certificate and private key provided by the key server. After you configure the trusted key provider, the key server accepts traffic from the trusted key provider.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.
- Request a certificate and private key in PEM format from the key server vendor. If the certificate is returned in a format other than PEM, convert it to PEM. If the private key is protected with a password, create a PEM file with the password removed. You can use the `openssl` command for both operations. For example:
  - To convert a certificate from CRT to PEM format:

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - To convert a certificate from DER to PEM format:

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

  - To remove the password from a private key:

    ```
    openssl rsa -in key.pem -out keynopassword.pem
    ```

```
Enter pass phrase for key.pem:
writing RSA key
```

1. Ensure that you are connected to the vCenter Server of the Trust Authority Cluster. For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

3. Assign the `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` information to a variable. For example:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   If you are following these tasks in order, you previously assigned `Get-TrustAuthorityCluster` information to a variable (for example, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   The `$kp` variable obtains the trusted key providers in the given Trust Authority Cluster, in this case, `$vTA` .

   Note: If you have more than one trusted key provider, use commands similar to the following to select the one you want:

   ```
   Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   <The trusted key providers listing is displayed.>
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
   ```

   Using `Select-Object -Last 1` selects the last trusted key provider in the list.

4. Upload the certificate and private key using the `Set-TrustAuthorityKeyProviderClientCertificate` command.

   For example:

   ```
   Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath <path/to/cert-
   file.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
   ```

The trusted key provider has established trust with the key server.

Create a Certificate Signing Request to Establish a Trusted Key Provider Trusted Connection

Some key server (KMS) vendors require that you generate a Certificate Signing Request (CSR) and send that CSR to the key server vendor. The key server vendor signs the CSR and returns the signed certificate. After you configure this signed certificate as the trusted key provider's client certificate, the key server accepts traffic that comes from the trusted key provider.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.

This task is a two-step process. First you generate the CSR and send it to your key server vendor. Then you upload the signed certificate that you receive from the key server vendor.

1. Ensure that you are connected to the vCenter Server of the Trust Authority Cluster. For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
```

3. Assign the `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` information to a variable. For example:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   If you are following these tasks in order, you previously assigned `Get-TrustAuthorityCluster` information to a variable (for example, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   This variable obtains the trusted key providers in the given Trust Authority Cluster, in this case, `$vTA` .

   Note: If you have more than one trusted key provider, use commands similar to the following to select the one you want:

   ```
   Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   <The trusted key providers listing is displayed.>
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
   ```

   Using `Select-Object -Last 1` selects the last trusted key provider in the list.

4. To generate a CSR, use the `New-TrustAuthorityKeyProviderClientCertificateCSR` cmdlet.

   For example:

   ```
   New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
   ```

   The CSR is displayed. You can also use the `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp` cmdlet to obtain the CSR.

5. To get a signed certificate, submit the CSR to your key server vendor.

   The certificate must be in PEM format. If the certificate is returned in a format other than PEM, convert it to PEM by using the `openssl` command. For example:

   - To convert a certificate from CRT to PEM format:

     ```
     openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
     ```

   - To convert a certificate from DER to PEM format:

     ```
     openssl x509 -inform DER -in clientcert.der -out clientcert.pem
     ```

6. When you receive the signed certificate from the key server vendor, upload the certificate to the key server using the `Set-TrustAuthorityKeyProviderClientCertificate` cmdlet.

   For example:

   ```
   Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath <path/tp/cert-file.pem>
   ```

The trusted key provider has established trust with the key server.

Export the Trust Authority Cluster Information

For the Trusted Cluster to connect to the vSphere Trust Authority Cluster, you must export the Trust Authority Cluster's service information in the form of a file then import that file to the Trusted Cluster. You must ensure to keep this file confidential and transport it securely.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.

If you are following these tasks in order, you are still connected to the vCenter Server of the Trust Authority Cluster.

Note: Store the exported service information file in a secure location, in case you must restore the vSphere Trust Authority configuration.

1. Ensure that you are connected to the vCenter Server of the Trust Authority Cluster. For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trust Authority Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

3. To export the Trust Authority Cluster's Attestation Service and Key Provider Service information, run the `Export-TrustAuthorityServicesInfo` cmdlet.
   For example, this command exports the service information to the `clsettings.json` file. If you are following these tasks in order, you previously assigned the `Get-TrustAuthorityCluster` information to a variable (for example, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath C:\vta\clsettings.json
   ```

   The file is created.

A file containing the Trust Authority Cluster information is created.

Export the Trust Authority Cluster Information

This example shows how to use PowerCLI to export the Trust Authority Cluster service information. The following table shows the example components and values that are used.

Table 264: Example vSphere Trust Authority Setup

Component	Value
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
vCenter Server for Trust Authority Cluster	192.168.210.22
Trust Authority administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User trustedadmin@v-
sphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -
FilePath C:\vta\clsettings.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/16/2019   9:59 PM           8177 clsettings.json
```

Continue with Import the Trust Authority Cluster Information to the Trusted Hosts.

Import the Trust Authority Cluster Information to the Trusted Hosts

After you have imported the vSphere Trust Authority Cluster information to the Trusted Cluster, the Trusted Hosts start the attestation process with the Trust Authority Cluster.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.

- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.
- Export the Trust Authority Cluster Information.

1. Ensure that you are connected as the Trust Authority administrator to the vCenter Server of the Trusted Cluster.
   For example, you can enter `$global:defaultviservers` to show all the connected servers.
2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trusted Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

   Note: Alternatively, you can start another PowerCLI session to connect to the vCenter Server of the Trusted Cluster.
3. Verify that the state of the Trusted Cluster is disabled.

   ```
   Get-TrustedCluster
   ```

   The State is shown as Disabled.
4. Assign the `Get-TrustedCluster` information to a variable.
   For example, this command assigns information for the cluster `Trusted Cluster` to the variable `$TC` .

   ```
   $TC = Get-TrustedCluster -Name 'Trusted Cluster'
   ```
5. Verify the value of the variable by echoing it.
   For example:

   ```
   $TC
   ```

   The `Get-TrustedCluster` information is displayed.
6. To import the Trust Authority Cluster information to the vCenter Server, run the `Import-TrustAuthorityServicesInfo` cmdlet.
   For example, this command imports the service information from the `clsettings.json` file previously exported in Export the Trust Authority Cluster Information.

   ```
   Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
   ```

   The system responds with a confirmation prompt.

   ```
   Confirmation
   Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

   [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
   ```
7. At the confirmation prompt, press Enter. (The default is `Y`.)
   The service information for the hosts in the Trust Authority Cluster is displayed.
8. To enable the Trusted Cluster, run the `Set-TrustedCluster` cmdlet.
   For example:

   ```
   Set-TrustedCluster -TrustedCluster $TC -State Enabled
   ```

   The system responds with a confirmation prompt.

   ```
   Confirmation
   Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
   [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
   ```

   If the Trusted Cluster is not in a healthy state, the following warning message is displayed before the confirmation message:

   ```
   WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus. This cmdlet will
    automatically remediate the TrustedCluster.
   ```

9. At the confirmation prompt, press Enter. (The default is `Y`.)

   The Trusted Cluster is enabled.

   Note: You can also enable the Trusted Cluster by enabling the Attestation Service and the Key Provider Service individually. Use the `Add-TrustedClusterAttestationServiceInfo` and `Add-TrustedClusterKeyProviderServiceInfo` commands. For example, the following commands enable the services one at a time for the cluster `Trusted Cluster` that has two Key Provider Services and two Attestation Services.

   ```
   Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster' -AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
   Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster' -KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
   ```

10. Verify that the Attestation Service and the Key Provider Service are configured in the Trusted Cluster.

    a) Assign the `Get-TrustedCluster` information to a variable.
    For example, this command assigns information for the cluster `Trusted Cluster` to the variable `$TC` .

    ```
    $TC = Get-TrustedCluster -Name 'Trusted Cluster'
    ```

    b) Verify that the Attestation Service is configured.

    ```
    $tc.AttestationServiceInfo
    ```

    The Attestation Service information is displayed.

    c) Verify that the Key Provider Service is configured.

    ```
    $tc.KeyProviderServiceInfo
    ```

    The Key Provider Service information is displayed.

The ESXi Trusted Hosts in the Trusted Cluster begin the attestation process with the Trust Authority Cluster.

Import the Trust Authority Cluster Information to the Trusted Hosts

This example shows how to import the Trust Authority Cluster service information to the Trusted Cluster. The following table shows the example components and values that are used.

Table 265: Example vSphere Trust Authority Setup

Component	Value
vCenter Server of the Trusted Cluster	192.168.110.22
Trust Authority administrator	trustedadmin@vsphere.local
Trusted Cluster name	Trusted Cluster
ESXi hosts in the Trust Authority Cluster	192.168.210.51 and 192.168.210.52
Variable `$TC`	`Get-TrustedCluster -Name 'Trusted Cluster'`

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User trustedadmin@v-sphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster
```

```
Name                 State            Id
----                 -----            --
Trusted Cluster      Disabled         TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                 State            Id
----                 -----            --
Trusted Cluster      Disabled         TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress               ServicePort         ServiceGroup
--------------               -----------         ------------
192.168.210.51               443                 host-13:86f7ab6c-ad6f-4606-...
192.168.210.52               443                 host-16:86f7ab6c-ad6f-4606-...
192.168.210.51               443                 host-13:86f7ab6c-ad6f-4606-...
192.168.210.52               443                 host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

Name                 State            Id
----                 -----            --
Trusted Cluster      Enabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress               ServicePort         ServiceGroup
--------------               -----------         ------------
192.168.210.51               443                 host-13:dc825986-73d2-463c-...
192.168.210.52               443                 host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress               ServicePort         ServiceGroup
--------------               -----------         ------------
192.168.210.51               443                 host-13:dc825986-73d2-463c-...
192.168.210.52               443                 host-16:dc825986-73d2-463c-...
```

Continue with Configure the Trusted Key Provider for Trusted Hosts Using the vSphere Client or Configure the Trusted Key Provider for Trusted Hosts Using the Command Line.

Configure the Trusted Key Provider for Trusted Hosts Using the vSphere Client

You can configure the trusted key provider by using the vSphere Client.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.
- Export the Trust Authority Cluster Information.
- Import the Trust Authority Cluster Information to the Trusted Hosts.

1. Connect to vCenter Server of the Trusted Cluster by using the vSphere Client.
2. Log in as the vCenter Server administrator, or an administrator that has the **Cryptographic operations** > **Manage key servers** privilege.
3. Select the vCenter Server, then select **Configure**.
4. Select **Key Providers** under **Security**.
5. Select **Add Trusted Key Providers**.

   The trusted key providers that are available are shown with a status of Connected.
6. Select a trusted key provider and click **Add Key Providers**.

   The trusted key provider is shown as Trusted and Connected. If this is the first trusted key provider that you add, it is marked as the default.

   Note: It takes a while for all the hosts to be able to get the key provider, and for the vCenter Server to update its cache. Because of the way the information is propagated, you might have to wait for a few minutes to use the key provider for key operations on some of the hosts.

ESXi Trusted Hosts can now perform cryptographic operations, such as creating encrypted virtual machines.

Encrypting a virtual machine with a trusted key provider looks the same as the virtual machine encryption user experience that was first delivered in vSphere 6.5. See Use Encryption in Your vSphere Environment.

Configure the Trusted Key Provider for Trusted Hosts Using the Command Line

You can configure trusted key providers by using the command line. You can configure the default trusted key provider for the vCenter Server, or at the cluster or the folder level in the vCenter object hierarchy.

- Enable the Trust Authority Administrator.
- Enable the Trust Authority State.
- Collect Information About ESXi Hosts and vCenter Server to Be Trusted.
- Import the Trusted Host Information to the Trust Authority Cluster.
- Create the Key Provider on the Trust Authority Cluster.
- Export the Trust Authority Cluster Information.
- Import the Trust Authority Cluster Information to the Trusted Hosts.

On the Trusted Cluster, you must have a role that includes the **Cryptographic operations** > **Manage KMS** privilege.

1. Ensure that you are connected as an administrator to the vCenter Server of the Trusted Cluster.

   For example, you can enter `$global:defaultviservers` to show all the connected servers.

2. Optional: If necessary, you can run the following commands to ensure that you are connected to the vCenter Server of the Trusted Cluster.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
   ```

3. Obtain the trusted key provider.

   ```
   Get-KeyProvider
   ```

   You can use the -Name*keyprovider* option to specify a single trusted key provider.

4. Assign the `Get-KeyProvider` trusted key provider information to a variable.
   For example, this command assigns the information to the variable `$workload_kp` .

   ```
   $workload_kp = Get-KeyProvider
   ```

   If you have multiple trusted key providers, you can use `Select-Object` to select one of them.

   ```
   $workload_kp = Get-KeyProvider | Select-Object -Index 0
   ```

5. Register the trusted key provider.

   ```
   Register-KeyProvider -KeyProvider $workload_kp
   ```

   To register additional trusted key providers, repeat Step 4 and Step 5.

   Note: It takes a while for all the hosts to be able to get the key provider, and for the vCenter Server to update its cache. Because of the way the information is propagated, you might have to wait for a few minutes to use the key provider for key operations on some of the hosts.

6. Set the default trusted key provider to use.
   a) To set the default key provider at the vCenter Server level, run the following command.

      ```
      Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
      ```

   b) To set the key provider at the cluster level, run the following command.
      For example, this command sets the key provider for the cluster `Trusted Cluster` .

      ```
      Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
      ```

   c) To set the key provider at the folder level, run the following command.
      For example, this command sets the key provider for the folder `TC Folder` , which was created on the `workLoad` data center.

      ```
      Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
      ```

Encrypting a virtual machine with a trusted key provider looks the same as the virtual machine encryption user experience that was first delivered in vSphere 6.5. See Use Encryption in Your vSphere Environment.

Managing vSphere Trust Authority in Your vSphere Environment

After you configure vSphere Trust Authority, you can perform additional operations, such as stopping and starting services, adding hosts to clusters, and viewing the status of the Trust Authority Cluster.

You can perform tasks by using the vSphere Client, the API, and the PowerCLI cmdlets. See *vSphere Web Services SDK Programming Guide*, the *VMware PowerCLI* documentation, and the *VMware PowerCLI Cmdlets Reference* documentation.

Start, Stop, and Restart vSphere Trust Authority Services

You can start, stop, and restart vSphere Trust Authority services by using the vSphere Client.

The services that make up vSphere Trust Authority are the Attestation Service (attestd) and the Key Provider Service (kmxd).

1. Connect to the vCenter Server of the vSphere Trust Authority Cluster by using the vSphere Client.
2. Log in as an administrator.
3. Browse to an ESXi host in the Trust Authority Cluster.
4. Select **Configure**, then select **Services** under **System**.
5. Locate the attestd service and the kmxd service.
6. Select the **Restart**, **Start**, or **Stop** operation as appropriate.

View the Trust Authority Hosts

You can view the vSphere Trust Authority hosts configured for a Trusted Cluster by using the vSphere Client.

1. Connect to the vCenter Server of the Trusted Cluster by using the vSphere Client.
2. Log in as an administrator.
3. Select the vCenter Server instance.
4. Click the **Configure** tab and select **Trust Authority** under **Security**.
   The ESXi hosts in the Trust Authority Cluster configured for the Trusted Cluster are displayed.

View the vSphere Trust Authority Cluster State

You can view the state of the vSphere Trust Authority Cluster by using the vSphere Client. The state is either enabled or disabled.

When the Trust Authority Cluster state is enabled, the Trusted Hosts in the Trusted Cluster can communicate with the Attestation Service and the Key Provider Service.

1. Connect to the vCenter Server of the Trust Authority Cluster by using the vSphere Client.
2. Log in as an administrator.
3. Select the Trust Authority Cluster in the object hierarchy.
4. Click the **Configure** tab and select **Trust Authority Cluster** under **Trust Authority**.
   The status displays as Enabled or Disabled.

Restart the Trusted Host Service

You can restart the service that runs on your Trusted Hosts.

Access to the ESXi shell must be enabled. See Enable Access to the ESXi Shell.

The service, kmxa, runs on the ESXi Trusted Hosts.

1. Use SSH or another remote console connection to start a session on the ESXi Trusted Host.
2. Log in as root.
3. Run the following command.

```
/etc/init.d/kmxa restart
```

Adding and Removing vSphere Trust Authority Hosts

You add and remove ESXi hosts to a vSphere Trust Authority Cluster by using VMware-supplied scripts.

In vSphere 7.0, you add and remove ESXi hosts to and from an existing vSphere Trust Authority Cluster or a Trusted Cluster by using VMware-supplied scripts. Starting in vSphere 7.0 Update 1, you use the remediate function to add ESXi hosts to an existing Trusted Cluster. See Add a Host to a Trusted Cluster with the vSphere Client and Add a Host to a Trusted Cluster with the CLI. In vSphere 7.0 Update 1, you still must use scripts to add ESXi hosts to an existing Trust Authority Cluster. See the VMware knowledge base articles at https://kb.vmware.com/s/article/77234 and https://kb.vmware.com/s/article/77146.

Add a Host to a Trusted Cluster with the vSphere Client

You can add ESXi hosts to an existing Trusted Cluster using the vSphere Client.

The vCenter Server for the Trusted Cluster must be running vSphere 7.0 Update 1 or later.

If you are adding an ESXi host that has a different ESXi version, or a different TPM hardware type, than what you initially configured for the Trusted Cluster, additional steps are required. You must export and import this information to the vSphere Trust Authority Cluster. See Collect Information About ESXi Hosts and vCenter Server to Be Trusted and Import the Trusted Host Information to the Trust Authority Cluster.

Required privileges: See the add hosts tasks in Required vCenter Server Privileges for Common Tasks.

After you have initially configured a Trusted Cluster, you might want to add more ESXi hosts. However, when you add the host to a Trusted Cluster, you must take the additional step of remediation. When you remediate the Trusted Cluster, you ensure that its desired configuration state matches its applied configuration.

In the first version of vSphere Trust Authority released in vSphere 7.0, you run scripts to add a host to an existing Trusted Cluster. Starting in vSphere 7.0 Update 1, you use the remediate functionality to add a host to a Trusted Cluster. In vSphere 7.0 Update 1, you still must use scripts to add a host to an existing Trust Authority Cluster. See Adding and Removing vSphere Trust Authority Hosts.

1. Connect to the vCenter Server of the Trusted Cluster by using the vSphere Client.
2. Log in as a Trust Authority administrator.
3. Navigate to a Trusted Cluster.
4. On the **Configure** tab, select **Configuration** > **Quickstart**.
5. Click **Add** in the **Add hosts** card.
6. Follow the prompts.
7. On the **Trust Authority** tab, click **Remediate**.
8. To verify that the Trusted Cluster is healthy, click **Check Health**.

Add a Host to a Trusted Cluster with the CLI

You can add ESXi hosts to an existing Trusted Cluster using the command line.

- The vCenter Server for the Trusted Cluster must be running vSphere 7.0 Update 1 or later.
- PowerCLI 12.1.0 or later is required.
- Required privileges: See the add hosts tasks in Required vCenter Server Privileges for Common Tasks.

After you have initially configured a Trusted Cluster, you might want to add more ESXi hosts. However, when you add the host to a Trusted Cluster, you must take the additional step of remediation. When you remediate the Trusted Cluster, you ensure that its desired configuration state matches its applied configuration.

In the first version of vSphere Trust Authority released in vSphere 7.0, you run scripts to add a host to an existing Trusted Cluster. Starting in vSphere 7.0 Update 1, you use the remediate functionality to add a Trusted Host. In vSphere 7.0 Update 1, you still must use scripts to add a host to an existing Trust Authority Cluster. See Adding and Removing vSphere Trust Authority Hosts.

1. Use whatever steps you normally do to add the ESXi host to the Trusted Cluster.
2. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as the Trust Authority administrator to the vCenter Server of the Trusted Cluster.

   ```
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

3. To check the Trusted Cluster's status, run the `Get-TrustedClusterAppliedStatus` PowerCLI cmdlet.

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
   ```

4. If the Trusted Cluster is not healthy, run the `Set-TrustedCluster` cmdlet with the `-Remediate` parameter.

   ```
   Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
   ```

5. To verify that the Trusted Cluster is healthy, rerun the `Get-TrustedClusterAppliedStatus` cmdlet.

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
   ```

Decommission Trusted Hosts from a Trusted Cluster

You can remove, or decommission, Trusted Hosts from a Trusted Cluster. You can decommission one or all Trusted Hosts from a Trusted Cluster, depending on the scenario.

- The vCenter Server for the Trusted Cluster must be running vSphere 7.0 Update 1 or later.
- If you use PowerCLI, version 12.1.0 or later is required.

When you decommission a Trusted Host, the remediate function sets the desired state of the Trusted Host to that of the non-Trusted Cluster where it is moved to. The decommissioned Trusted Host becomes a regular host. The Trusted Cluster (from where the Trusted Host was moved) continues to have its desired state configuration and functions still as a Trusted Cluster.

When you remove all the Trusted Hosts from a Trusted Cluster, you decommission the Trusted Cluster. You remove both the desired state configuration and applied configuration from the Trusted Hosts and the Trusted Cluster, then move all the Trusted Hosts to a non-Trusted Cluster.

You can reuse decommissioned Trusted Hosts in your environment. For example you can reuse the hosts in a non-trusted infrastructure capacity, or as vSphere Trust Authority Hosts. You can use the decommissioned hosts in the same vCenter Server or a different vCenter Server.

For more information about Trusted Cluster configuration and health, see Trusted Cluster Health and Remediation Overview.

1. Connect to the vCenter Server of the Trusted Cluster by using the vSphere Client.
2. Log in as a Trust Authority administrator.
3. Navigate to a Trusted Cluster.
4. Decide how to decommission the Trusted Hosts from the Trusted Cluster.

Task	Steps
Keep the desired configuration state of the Trusted Cluster and the remaining Trusted Hosts	1. Put hosts into Maintenance mode and move them to a new, empty cluster (that is, the cluster does not contain any hosts). 2. Exit Maintenance mode on the hosts.

Task	Steps
	3. For the new, empty cluster (not the Trusted Cluster), on the **Trust Authority** tab, click **Remediate**. Remediation removes the Trusted configuration from the moved hosts. The Trusted Cluster retains its desired state configuration.

Remove the desired configuration state and applied configuration state of all the Trusted Hosts	1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as the Trust Authority administrator to the vCenter Server of the Trusted Cluster.
	`Connect-VIServer -server TrustedCluster-ter_VC_ip_address -User trust_admin_user -Password 'password'`
	2. Run the `Set-TrustedCluster` cmdlet, for example:
	`Set-TrustedCluster -TrustedCluster 'Trusted-Cluster' -State Disabled`
	The Trusted Infrastructure configuration is removed from all the Trusted Hosts, and the Trusted Cluster has its desired state configuration removed.
	3. Put all hosts into Maintenance mode and move them to a different cluster.
	4. Exit Maintenance mode on the hosts.

5. To verify that the Trusted Cluster is healthy, click **Check Health** on the **Trust Authority** tab for the Trusted Cluster.

If you no longer plan to attest the specific versions of ESXi or the TPM hardware from the decommissioned ESXi hosts, update the Trust Authority Cluster's configuration, for optimal security. See the VMware knowledge base article at https://kb.vmware.com/s/article/77146.

Backing Up the vSphere Trust Authority Configuration

Use the files you exported when configuring vSphere Trust Authority as your Trust Authority backup. You can use these files to restore a Trust Authority deployment. Keep these configuration files confidential and transport them securely.

Most vSphere Trust Authority configuration and state information is stored on the ESXi hosts in the ConfigStore database. The vCenter Server Management Interface that you use to back up a vCenter Server instance does not back up the configuration information for vSphere Trust Authority. If you save and securely store the configuration files that you exported when setting up your vSphere Trust Authority environment, then you have the necessary information to restore a vSphere Trust Authority configuration. See Collect Information About ESXi Hosts and vCenter Server to Be Trusted if you must generate this information.

Change the Primary Key of a Key Provider

You can change the primary key of a key provider, for example, when you want to rotate the primary key that is used.

Create and activate a key on the key server (KMS) to be used as the new primary key for the trusted key provider. This key wraps other keys and secrets used by this trusted key provider. See your KMS vendor documentation for more information about creating keys.

See Virtual Machine Encryption Best Practices for guidance about key life cycle.

1. Run the `Set-TrustAuthorityKeyProvider` command.
   For example:
   `Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID`

2. Verify the status of the key provider.
   a) Assign `Get-TrustAuthorityCluster` information to a variable.
      For example:
      ```
      $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
      ```
   b) Assign the `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` information to a variable.
      For example:
      ```
      $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
      ```
   c) Verify the status of the key provider by running `$kp.Status`.
      For example:
      ```
      $kp.Status

      KeyProviderId Health HealthDetails ServerStatus
      ------------- ------ ------------- ------------
      domain-c8-kp4     Ok {}            {IP_address}
      ```
      A Health status of Ok indicates that the key provider is running correctly.

The new primary key is used for any new encryption operations. Data encrypted with the old primary key is still decrypted using the old key.

Trusted Host Attestation Reporting Overview

In vSphere Trust Authority, vCenter Server verifies and reports on a Trusted Host's attestation status. You can use the vSphere Client to view the attestation status of Trusted Hosts.

vSphere Trust Authority uses remote attestation for Trusted Hosts to prove the authenticity of their booted software. Attestation verifies that the Trusted Hosts are running authentic VMware software, or VMware-signed partner software. The vCenter Server of the Trusted Cluster communicates with the Trusted Host to get an internal attestation report. The attestation report specifies if the Trusted Host has attested or not with the Attestation Service running on the Trust Authority Cluster. If the Trusted Host has not attested, the attestation report also specifies an error message. The vSphere Client displays the following attestation statuses for Trusted Hosts.

Passed	The Trusted Host has attested with a vSphere Trust Authority Attestation Service, and the internal attestation report is available to vCenter Server.
Failed	The Trusted Host was not able to attest with any vSphere Trust Authority Attestation Service. The vCenter Server internal attestation report contains the error reported by the Attestation Service that the Trusted Host tried to attest with.

The vSphere Client also displays if a host was attested by vSphere Trust Authority or by vCenter Server.

When a Trusted Host is unattested, virtual machines, including encrypted virtual machines, that are running on the Trusted Host continue to be accessible. You cannot power on virtual machines on an unattested Trusted Host. However, you can still add unencrypted virtual machines. When a Trusted Host is unattested, take steps to resolve the attestation problem. For more information about attestation concepts, see vSphere Trust Authority Process Flows.

When you have configured multiple Trust Authority Hosts, there are potentially multiple attestation reports available from each host. When reporting status, the vSphere Client displays the status from the first "attested" report that it finds. If there are no "attested" reports, the vSphere Client displays the error from the first "unattested" report that it finds.

Even if you have configured multiple Trust Authority Hosts, the vSphere Client displays the status, and potentially an error message, from only one attestation report.

View the Trusted Cluster Attestation Status

You can view the attestation status of a Trusted Host by using the vSphere Client.

- Both the Trusted Hosts and the vSphere Trust Authority hosts must be running ESXi 7.0 Update 1 or later.
- The vCenter Server hosts for the respective clusters must be running vSphere 7.0 Update 1 or later.

1. Connect to the vCenter Server of the Trusted Cluster by using the vSphere Client.
2. Log in as an administrator.
   You can log in as a Trust Authority administrator or vSphere administrator.
3. Navigate to a data center and click the **Monitor** tab.
4. Click **Security**.
5. Review the Trusted Host's status in the Attestation column and read the accompanying message in the Message column.

If there are errors, see Troubleshoot Trusted Host Attestation Problems.

Troubleshoot Trusted Host Attestation Problems

The vSphere Trust Authority attestation reporting provides a starting point for troubleshooting Trusted Host attestation errors.

1. View the Trusted Cluster Attestation Status.
2. Use the following table to troubleshoot and resolve errors.

Error	Cause and Solution
Attestation Services not configured.	Attestation Services have not been configured. Configure the Trusted Host to use attestation services by using the Remediate action. See Remediate a Trusted Cluster.
No TPM2 device available.	Install and configure the Trusted Host to use a Trusted Platform Module (TPM). See your vendor documentation.
TPM2 endorsement public key or certificate could not be retrieved.	Check that the TPM is supported, and that it has a valid endorsement key. You might need to contact VMware Support.
Attestation report is not available.	It is possible that the Trusted Host has not finished attestation. Wait a few minutes then recheck the attestation status.
Attestation Service version is incompatible with the request.	Update the Trust Authority host running the Attestation Service to vSphere 7.0 Update 1 or later.
Attestation failed because Secure Boot is not enabled.	Check that the Trusted Host is configured to use Secure Boot. See UEFI Secure Boot for ESXi Hosts.
Attestation failed to identify the remote software version.	Import the Trusted Host's base image information to the Attestation Service. See Import the Trusted Host Information to the Trust Authority Cluster.
Attestation failed because a TPM certificate is required.	Check that the TPM is supported. Alternatively, run the following PowerCLI cmdlet to modify the com.vmware.esx.attestation.tpm2.settings to set `requireCertificateValidation` to `false`. `Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:$false -RequireEndorsementKey:$true`
Attestation failed due to an unknown TPM.	Import the TPM endorsement key to the Attestation Services. See Import the Trusted Host Information to the Trust Authority Cluster.

Error	Cause and Solution
Error: vapi.send.failed.	The kmxa service might not be running on the Trusted Host or the kmxa service cannot contact the Attestation Service. Ensure that the kmxa service is started. Also, check that the Attestation Service is running. See Restart the Trusted Host Service.

Checking and Remediating Trusted Cluster Health

You can check and validate the health of a Trusted Cluster. When problems arise with the health of a Trusted Cluster, you can remediate a Trusted Cluster's configuration.

Trusted Cluster Health and Remediation Overview

If a Trusted Cluster's configuration is not healthy, you must resolve the configuration inconsistencies. You do so by remediating the Trusted Cluster. When you remediate a Trusted Cluster, you ensure that all the Trusted Hosts in the Trusted Cluster have the same trusted configuration.

A Trusted Cluster consists of a vCenter Server cluster of Trusted ESXi Hosts that are remotely attested by the Trust Authority Cluster. When you configure vSphere Trust Authority initially, you must import the Trust Authority Services information from your Trust Authority Cluster into the Trusted Cluster. The Trusted Cluster uses that configuration of components for contacting the Key Provider Service and the Attestation Service running on the Trust Authority Cluster. For more information about configuring a Trusted Cluster, see Import the Trust Authority Cluster Information to the Trusted Hosts. After you configure a Trusted Cluster, you can check and remediate its health.

Trusted Cluster Health Overview

Checking the health of a Trusted Cluster depends upon the following.

Desired state configuration	The desired state configuration is based on the Trust Authority Services information that you import into the Trusted Cluster. The desired state configuration is the Trusted Cluster's "source of truth." Think of the desired state configuration as what is initially created when you set up the Trusted Cluster.
Applied configuration	The applied configuration is the registration of the specific Attestation Services and Key Provider Services for which you have configured the Trusted Cluster. The applied configuration is what the Trusted Cluster is running currently. You can think of the applied configuration as the "run-time" configuration. The desired state configuration should match the applied configuration. However, if the applied configuration is inconsistent with the desired state configuration, the Trusted Cluster is deemed "not healthy." A Trusted Cluster that is not healthy can experience degraded performance or not function at all.

This health check is not an indicator of the overall health for either a Trusted Cluster or the vSphere Trust Authority infrastructure. The health check only compares the Trusted Cluster's desired state configuration to the applied configuration.

Trusted Cluster Remediation Overview

Remediation is the process by which vSphere Trust Authority resolves an inconsistent configuration of a Trusted Cluster. A Trusted Cluster's configuration can become inconsistent over time or due to other operational errors.

Use remediation in the following way:

- Check the Trusted Cluster health.

- If the Trusted Cluster is unhealthy, remediate it.

You can use either the vSphere Client or the CLI to check the Trusted Cluster health. See Check Trusted Cluster Health. You can also use either the vSphere Client or the CLI to remediate a Trusted Cluster. See Remediate a Trusted Cluster.

Note: Remediation is also the appropriate process to use when you add a host to an existing Trusted Cluster. See Add a Host to a Trusted Cluster with the vSphere Client and Add a Host to a Trusted Cluster with the CLI.

Check Trusted Cluster Health

You can check the health status of a Trusted Cluster by using either the vSphere Client or the command line.

- The vCenter Server for the Trusted Cluster must be running vSphere 7.0 Update 1 or later.
- If you use PowerCLI, version 12.1.0 or later is required.

For more information, see Trusted Cluster Health and Remediation Overview.

1. Check the Trusted Cluster health.

Tool	Steps
vSphere Client	1. Connect to the vCenter Server of the Trusted Cluster by using the vSphere Client. 2. Log in as a Trust Authority administrator. 3. Navigate to a Trusted Cluster, select **Configure**, then select **Trust Authority**. 4. Click **Check Health**.

CLI	1. In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as the Trust Authority administrator to the vCenter Server of the Trusted Cluster.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	2. Run the `Get-TrustedClusterAppliedStatus` cmdlet, for example:
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

2. If there are errors, see Remediate a Trusted Cluster.

Remediate a Trusted Cluster

You can remediate the configuration of a Trusted Cluster by using either the vSphere Client or the command line.

The vCenter Server for the Trusted Cluster must be running vSphere 7.0 Update 1 or later.

1. Connect to the vCenter Server of the Trusted Cluster.

Tool	Steps
vSphere Client	1. Connect to the vCenter Server of the Trusted Cluster by using the vSphere Client. 2. Log in as a Trust Authority administrator.
CLI	In a PowerCLI session, run the `Connect-VIServer` cmdlet to connect as the Trust Authority administrator to the vCenter Server of the Trusted Cluster. `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`

2. Remediate the Trusted Cluster then recheck the Trusted Cluster health.

Tool	Steps
vSphere Client	1. Navigate to a Trusted Cluster. 2. Select **Configure**, then select **Trust Authority**. 3. Click **Remediate**. 4. Click **Check Health**.

CLI	1. Run the `Set-TrustedCluster` cmdlet with the `-Remediate` parameter, for example:
	`Set-TrustedCluster -TrustedCluster 'Trusted-Cluster' -Remediate`
	2. Run the `Get-TrustedClusterAppliedStatus` cmdlet, for example:
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

Use Encryption in Your vSphere Environment

Whether you use a standard key provider, trusted key provider, or vSphere Native Key Provider, using encryption in your vSphere environment requires some preparation.

After your environment is set up, you can use the vSphere Client to create encrypted virtual machines and virtual disks and encrypt existing virtual machines and disks.

You can perform additional tasks by using the API and by using the `crypto-util` CLI. See the *vSphere Web Services SDK Programming Guide* for the API documentation and the `crypto-util` command-line help for details about that tool.

Create an Encryption Storage Policy

Before you can create encrypted virtual machines, you must create an encryption storage policy. You create the storage policy once, and assign it each time you encrypt a virtual machine or virtual disk.

- Set up the connection to a key provider.
  Although you can create a VM Encryption storage policy without the key provider connection in place, you cannot perform encryption tasks until trusted connection with the key provider is established.
- Required privileges: **Cryptographic operations** > **Manage encryption policies**.

If you want to use virtual machine encryption with other I/O filters, or to use the **Create VM Storage Policy** wizard in the vSphere Client, see the *vSphere Storage* documentation for details.

1. Log in to the vCenter Server by using the vSphere Client.
2. Select **Home**, click **Policies and Profiles**, then click **VM Storage Policies**.
3. Click **Create**.
4. Select the vCenter Server, enter a policy name, optionally enter a description, then click **Next**.
5. On the **Policy structure** page, check **Enable host based roles** then click **Next**.
6. On the **Host based services** page, select **Use storage policy component**, choose **Default encryption properties** from the drop-down menu, then click **Next**.
7. On the **Storage compatibility** page, leave **Compatible** selected, select a datastore, then click **Next**.
8. Review the information and click **Finish**.

The VM Encryption storage policy is added to the list, and is available for use when encrypting a virtual machine.

Enable Host Encryption Mode Explicitly

Host encryption mode must be enabled if you want to perform encryption tasks, such as creating an encrypted virtual machine, on an ESXi host. In most cases, host encryption mode is enabled automatically when you perform an encryption task.

Required privilege: **Cryptographic operations.Register host**

Sometimes, turning on encryption mode explicitly is necessary. See Prerequisites and Required Privileges for Encryption Tasks.

1. Log in to the vCenter Server by using the vSphere Client.
2. Browse to the ESXi host and click **Configure**.
3. Under System, click **Security Profile**.
4. Click **Edit** in the Host Encryption Mode panel.
5. Select **Enabled** and click **OK**.

Disable Host Encryption Mode Using the API

Host encryption mode is enabled automatically when you perform an encryption task, if the user has sufficient privilege to enable the encryption mode. After host encryption mode is enabled, all core dumps are encrypted to avoid the release of sensitive information to support personnel. If you no longer use virtual machine encryption with an ESXi host, you can disable encryption mode.

After encryption mode is enabled for an ESXi host, you might need to disable it. For example, you might need to disable encryption mode to generate an ESXi support bundle (using the `vm-support` command). Using the Disable Host Encryption mode toggle (**Host** > **Configure** > **Security Profile** > **Edit Host Encryption Mode**) does not work when key material exists on the host.

You can use the API to disable host encryption mode by invoking the `CryptoManagerHostDisable` API method.

The crypto modes, or states, defined for an ESXi host are:

- pendingIncapable: The host is crypto disabled, that is, the host cannot perform vSphere Virtual Machine Encryption operations.
- incapable: The host is not safe for receiving sensitive material.
- prepared: The host is prepared for receiving sensitive material but does not have a host key set yet.
- safe: The host is crypto safe (enabled), and has a host key set, that is, vSphere Virtual Machine Encryption operations are possible.

After you invoke `CryptoManagerHostDisable` on a host, the crypto state of the host changes as follows:

- If the original host crypto state is incapable or prepared, the host crypto state is changed to incapable.
- If the original host crypto state is safe, the host crypto state is changed to pendingIncapable.
- If the host crypto state is pendingIncapable, the host crypto state is still pendingIncapable.

This task shows how to disable host encryption mode by using the vCenter Server Managed Object Browser (MOB). For more information about using the API, see the *vSphere Web Services API* documentation at https://developer.vmware.com/apis/968/vsphere.

1. Log in to the vCenter Server as an administrator.
2. Unregister all encrypted virtual machines from the ESXi host whose encryption mode you want to disable.
3. Access the MOB on the vCenter Server.

   `https://vcenter_server/mob`

4. Invoke the `CryptoManagerHostDisable` method on a host.
   a) Under content name, click **content**.
   b) Under rootFolder, click **group-D1 (Datacenters)**.
   c) Under childEntity, click the appropriate datacenter.
   d) Under hostFolder, click the appropriate host.
   e) Under childEntity, click the appropriate cluster.
   f) Under host, click the appropriate host.
   g) Under configManager, click **configManager**.
   h) Under cryptoManager, click **CryptoManagerHost-***number*.
   i) Click **CryptoManagerHostDisable**.
   The host crypto state is changed to either pendingIncapable or incapable, depending on its original crypto state.
5. Repeat step 4 for other hosts on which you want to disable encryption mode.
6. Reboot the hosts.

Once the host encryption mode is disabled, you cannot perform encryption operations, such as adding encrypted virtual machines, unless you re-enable the host encryption mode.

Note: After you reboot an ESXi host on which you disabled encryption mode, if the host crypto state was originally pendingIncapable, the host crypto state is still pendingIncapable. To re-enable host encryption mode, re-access the vCenter Server MOB and invoke the `ConfigureCryptoKey` API method. When re-enabling host encryption mode, use the original host key ID if the host crypto state is pendingIncapable.

Create an Encrypted Virtual Machine

After you set up the KMS, you can create encrypted virtual machines.

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Ensure that the virtual machine is powered off.
- Verify that you have the required privileges:
  - **Cryptographic operations** > **Encrypt new**
  - If the host encryption mode is not Enabled, you also need **Cryptographic operations** > **Register host**.

This task describes how to create an encrypted virtual machine using the vSphere Client. The vSphere Client filters by virtual machine encryption storage policies, easing creation of encrypted virtual machines.

Note: Creating an encrypted virtual machine is faster and uses fewer storage resources than encrypting an existing virtual machine. If possible, encrypt virtual machines during the creation process.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object and select **New Virtual Machine**.
4. Follow the prompts to create an encrypted virtual machine.

Option	Action
Select a creation type	Create a new virtual machine.
Select a name and folder	Specify a unique name and target location for the virtual machine.
Select a compute resource	Specify an object for which you have privileges to create encrypted virtual machines. See Prerequisites and Required Privileges for Encryption Tasks.

Option	Action
Select storage	Select the **Encrypt this virtual machine** check box. Virtual machine storage policies that include encryption appear. Select a virtual machine storage policy (the bundled sample is VM Encryption Policy), and select a compatible datastore.
Select compatibility	Select the compatibility. You can migrate an encrypted virtual machine only to hosts with compatibility ESXi 6.5 and later.
Select a guest OS	Select a guest OS that you plan to install on the virtual machine later.
Customize hardware	Customize the hardware, for example, by changing disk size or CPU. (Optional) Select the **VM Options** tab, and expand **Encryption**. Select which disks to exclude from encryption. When you deselect a disk, only the VM Home and any other selected disks are encrypted. Any New Hard disk that you add is encrypted. You can change the storage policy for individual hard disks later.
Ready to complete	Review the information and click **Finish**.

Clone an Encrypted Virtual Machine

When you clone an encrypted virtual machine, the clone is encrypted with the same keys. To change keys for the clone, perform a recrypt of the clone using the API. See *vSphere Web Services SDK Programming Guide*.

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Required privileges:
  - **Cryptographic operations** > **Clone**
  - **Cryptographic operations** > **Encrypt**
  - **Cryptographic operations** > **Decrypt**
  - **Cryptographic operations** > **Recrypt**
  - If the host encryption mode is not Enabled, you also must have **Cryptographic operations** > **Register host** privileges.

You can perform the following operations during clone.

- Create an encrypted virtual machine from an unencrypted virtual machine or template virtual machine.
- Create a decrypted virtual machine from an encrypted virtual machine or template virtual machine.
- Recrypt the destination virtual machine with different keys from that of source virtual machine.

You can create an instant clone virtual machine from an encrypted virtual machine with the caveat that the instant clone shares the same key with the source virtual machine. You cannot recrypt keys on either the source or the instant clone virtual machine. See *vSphere Web Services SDK Programming Guide*.

1. Browse to the virtual machine in the vSphere Client inventory.
2. To create a clone of an encrypted machine, right-click the virtual machine, select **Clone** > **Clone to Virtual Machine**, and follow the prompts.

Option	Action
Select a name and folder	Specify a name and target location for the clone.
Select a compute resource	Specify an object for which you have privileges to create encrypted virtual machines. See Prerequisites and Required Privileges for Encryption Tasks.

Option	Action
Select storage	Make a selection in the **Select virtual disk format** menu and select a datastore. You can change the storage policy as part of the clone operation. For example, changing from using an encryption policy to a non-encryption policy decrypts the disks.
Select clone options	Select clone options, as discussed in the *vSphere Virtual Machine Administration* documentation.
Ready to complete	Review the information and click **Finish**.

3. Optional: Change the keys for the cloned virtual machine.

   By default, the cloned virtual machine is created with the same keys as its parent. Best practice is to change the cloned virtual machine's keys to ensure that multiple virtual machines do not have the same keys.

   a) Decide upon a shallow or deep recrypt.

      To use a different DEK and KEK, perform a deep recrypt of the cloned virtual machine. To use a different KEK, perform a shallow recrypt of the cloned virtual machine. For a deep recrypt, you must power off the virtual machine. You can perform a shallow recrypt operation while the virtual machine is powered on, and if the virtual machine has snapshots present. Shallow recrypt of an encrypted virtual machine with snapshots is permitted only on a single snapshot branch (disk chain). Multiple snapshot branches are not supported. If the shallow recrypt fails before updating all links in the chain with the new KEK, you can still access the encrypted virtual machine if you have the old and new KEKs.

   b) Perform a recrypt of the clone using the API. See *vSphere Web Services SDK Programming Guide*.

Encrypt an Existing Virtual Machine or Virtual Disk

You can encrypt an existing virtual machine or virtual disk by changing its storage policy. You can encrypt virtual disks only for encrypted virtual machines.

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Ensure that the virtual machine is powered off.
- Verify that you have the required privileges:
  - **Cryptographic operations** > **Encrypt new**
  - If the host encryption mode is not Enabled, you also need **Cryptographic operations** > **Register host**.

This task describes how to encrypt an existing virtual machine or virtual disk using the vSphere Client.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine that you want to change and select **VM Policies** > **Edit VM Storage Policies**.

   You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.
3. Select the storage policy.

   - To encrypt the VM and its hard disks, select an encryption storage policy and click **OK**.
   - To encrypt the VM but not the virtual disks, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.

   You cannot encrypt the virtual disk of an unencrypted VM.

4. If you prefer, you can encrypt the virtual machine, or both virtual machine and disks, from the **Edit Settings** menu in the vSphere Client.
   a) Right-click the virtual machine and select **Edit Settings**.
   b) Select the **VM Options** tab, and open **Encryption**. Choose an encryption policy. If you deselect all disks, only the VM home is encrypted.
   c) Click **OK**.

Decrypt an Encrypted Virtual Machine or Virtual Disk

You can decrypt a virtual machine, its disks, or both, by changing the storage policy.

- The virtual machine must be encrypted.
- The virtual machine must be powered off or in maintenance mode.
- Required privileges: **Cryptographic operations** > **Decrypt**

This task describes how to decrypt an encrypted virtual machine using the vSphere Client.

All encrypted virtual machines require encrypted vMotion. During virtual machine decryption, the Encrypted vMotion setting remains. To change this setting so that Encrypted vMotion is no longer used, change the setting explicitly.

This task explains how to perform decryption using storage policies. For virtual disks, you can also perform decryption using the **Edit Settings** menu.

Note: In the Virtual Machine Details pane, a vTPM-enabled virtual machine displays both a lock icon and an "Encrypted with *`key_provider`*" message. To remove a vTPM from a virtual machine, see Remove Virtual Trusted Platform Module from a Virtual Machine.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine that you want to change and select **VM Policies** > **Edit VM Storage Policies**.

   You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.
3. Select a storage policy.
   - To decrypt the VM and its hard disks, toggle off **Configure per disk**, select a storage policy from the drop-down menu, and click **OK**.
   - To decrypt a virtual disk but not the virtual machine, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.

   You cannot decrypt the virtual machine and leave the disk encrypted.

4. If you prefer, you can use the vSphere Client to decrypt the virtual machine and disks from the **Edit Settings** menu.
   a) Right-click the virtual machine and select **Edit Settings**.
   b) Select the **VM Options** tab and expand **Encryption**.
   c) To decrypt the VM and its hard disks, choose **None** from the **Encrypt VM** drop-down menu.
   d) To decrypt a virtual disk but not the virtual machine, deselect the disk.
   e) Click **OK**.
5. Optional: You can change the Encrypted vMotion setting.
   a) Right-click the virtual machine and click **Edit Settings**.
   b) Click **VM Options**, and open **Encryption**.
   c) Set the **Encrypted vMotion** value.

Change the Encryption Policy for Virtual Disks

When you create an encrypted virtual machine from the vSphere Client, you can select which virtual disks that you add during virtual machine creation are encrypted. You can decrypt virtual disks that are encrypted by using the **Edit VM Storage Policies** option.

- You must have the **Cryptographic operations** > **Manage encryption policies** privilege.
- Ensure that the virtual machine is powered off.

Note: An encrypted virtual machine can have virtual disks that are not encrypted. However, an unencrypted virtual machine cannot have encrypted virtual disks.

See Virtual Disk Encryption.

This task describes how to change the encryption policy using storage policies. You can also use the **Edit Settings** menu to make this change.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine and select **VM Policies** > **Edit VM Storage Policies** .
3. Change the storage policy.
   - To change the storage policy for the VM and its hard disks, select an encryption storage policy and click **OK**.
   - To encrypt the VM but not the virtual disks, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.

   You cannot encrypt the virtual disk of an unencrypted VM.
4. If you prefer, you can change the storage policy from the **Edit Settings** menu.
   a) Right-click the virtual machine and select **Edit Settings**.
   b) Select the **Virtual Hardware** tab, expand a hard disk, and select an encryption policy from the drop-down menu.
   c) Click **OK**.

Resolve Missing Key Issues

If the ESXi host cannot get the key (KEK) from vCenter Server for an encrypted virtual machine or an encrypted virtual disk, the encrypted VM becomes locked. After you make the keys available on the KMS, you can unlock a locked encrypted virtual machine.

Under certain circumstances when using a standard key provider, the ESXi host cannot get the key encryption key (KEK) for an encrypted virtual machine or an encrypted virtual disk from vCenter Server. In that case, you can still unregister or reload the virtual machine. However, you cannot perform other virtual machine operations such as powering on the virtual machine. After taking the necessary steps to make the required keys available on the KMS, you can unlock a locked encrypted virtual machine by using the vSphere Client.

If the virtual machine key is not available, a vCenter Server alarm notifies you and the state of the virtual machine displays as invalid. The virtual machine cannot power on. If the virtual machine key is available, but a key for an encrypted disk is not available, the virtual machine state does not display as invalid. However, the virtual machine cannot power on and the following error results:

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

Note: The following procedure illustrates the situations that can cause a virtual machine to become locked, the corresponding alarms and event logs that appear, and what to do in each case.

1. If the problem is the connection between the vCenter Server system and the KMS, vCenter Server generates a virtual machine alarm. Also, an error message appears in the event log.

   Restore the connection to the KMS. When the KMS and keys become available, unlock the locked virtual machines. See Unlock Locked Virtual Machines. You can also reboot the host and re-register the virtual machine to unlock it after restoring the connection.

   Losing the connection to the KMS does not automatically lock the virtual machine. The virtual machine only enters a locked state if the following conditions are met:

   - The key is not available on the ESXi host.
   - vCenter Server cannot retrieve keys from the KMS.

   After each reboot, the ESXi host must be able to reach vCenter Server. vCenter Server requests the key with the corresponding ID from the KMS and makes it available to ESXi.

   Note: In vSphere 7.0 Update 2 and later, you can persist encryption keys across ESXi reboots. See Key Persistence Overview.

   If, after restoring connection to the key provider, the virtual machine remains locked, see Unlock Locked Virtual Machines.

2. If the connection is restored, register the virtual machine. If an error results, or if the operation succeeds but the virtual machine is in a locked state, verify that you have the **Cryptographic operations** > **RegisterVM** privilege for the vCenter Server system.

   This privilege is not required for powering on an encrypted virtual machine if the key is available. This privilege is required for registering the virtual machine if the key has to be retrieved.

3. If the key is no longer available on the KMS, vCenter Server generates a virtual machine alarm. Also, an error message appears in the event log.

   Ask the KMS administrator to restore the key. You might encounter an inactive key if you are powering on a virtual machine that had been removed from the inventory and that had not been registered for a long time. It also happens if you reboot the ESXi host, and the KMS is not available.

   a) Retrieve the key ID by using the Managed Object Browser (MOB) or the vSphere API.

      Retrieve the `keyId` from `VirtualMachine.config.keyId.keyId`.

   b) Ask the KMS administrator to reactivate the key that is associated with that key ID.

   c) After restoring the key, see Unlock Locked Virtual Machines.

   If the key can be restored on the KMS, vCenter Server retrieves it and pushes it to the ESXi host the next time it is needed.

4. If the KMS is accessible and the ESXi host is powered on, but the vCenter Server system is unavailable, follow these steps to unlock virtual machines.

   a) Restore the vCenter Server system, or set up a different vCenter Server system, then establish trust with the KMS.

      You must use the same key provider name, but the KMS IP address can be different.

   b) Reregister all virtual machines that are locked.

      The new vCenter Server instance retrieves the keys from the KMS and the virtual machines are unlocked.

5. If the keys are missing only on the ESXi host, vCenter Server generates a virtual machine alarm and the following message appears in the event log:

   ```
   Virtual machine is locked because keys are missing on host.
   ```

   The vCenter Server system can retrieve the missing keys from the key provider. No manual recovery of keys is required. See Unlock Locked Virtual Machines.

Unlock Locked Virtual Machines

A vCenter Server alarm notifies you when an encrypted virtual machine is in a locked state. You can unlock a locked encrypted virtual machine by using the vSphere Client (HTML5-based client) after taking the necessary steps to make the required keys available on the KMS.

- Verify that you have the required privileges: **Cryptographic operations.RegisterVM**
- Other privileges might be required for optional tasks such as enabling host encryption.
- Before unlocking a locked virtual machine, troubleshoot the cause of the lock and attempt to fix the problem manually. See Resolve Missing Key Issues.

1. Connect to vCenter Server by using the vSphere Client.
2. Navigate to the virtual machine's **Summary** tab.

   When a virtual machine is locked, the Virtual Machine Locked alarm appears.
3. Decide if you want to either acknowledge the alarm, or reset the alarm to green but not unlock the virtual machine now.

   When you click either **Acknowledge** or **Reset to green**, the alarm goes away, but the virtual machine remains locked until you unlock it.
4. Navigate to the **Monitor** tab of the virtual machine and click **Events**.

   The **Events** pane displays information about why the virtual machine is locked.
5. Perform suggested troubleshooting before you unlock the virtual machine.
6. Navigate to the **Summary** tab of the virtual machine.

   A Virtual Machine Locked Alarm appears.
7. Select **Unlock VM** from the **Actions** drop-down menu on the right side.

Resolve ESXi Host Encryption Mode Issues

Under certain circumstances, the ESXi host's encryption mode can become disabled.

An ESXi host requires that host encryption mode is enabled if it contains any encrypted virtual machines. If the host detects it is missing its host key, or if the key provider is unavailable, the host might fail to enable the encryption mode. vCenter Server generates an alarm when the host encryption mode cannot be enabled.

1. If the problem is the connection between the vCenter Server system and the key provider, an alarm is generated and an error message appears in the event log.

   You must restore the connection to the key provider that contains the encryption keys in question.
2. If keys are missing, an alarm is generated and an error message appears in the event log.

   You must ensure that the keys are present in the key provider. Consult the documentation for your key management vendor for information about restoring from backup.

If, after restoring connection to the key provider, or manually recovering keys to the key provider, the host's encryption mode remains disabled, re-enable the host encryption mode. See Re-Enable ESXi Host Encryption Mode.

Re-Enable ESXi Host Encryption Mode

Starting with vSphere 6.7, a vCenter Server alarm notifies you when an ESXi host's encryption mode has become disabled. You can re-enable the host encryption mode if it has become disabled.

- Verify that you have the required privileges: **Cryptographic operations** > **Register host**
- Before re-enabling encryption mode, troubleshoot the cause and attempt to fix the problem manually.

1. Connect to vCenter Server by using the vSphere Client.
2. Navigate to the ESXi host's **Summary** tab.
   When the encryption mode is disabled, the Host Requires Encryption Mode Enabled alarm appears.
3. Decide if you want to either acknowledge the alarm, or reset the alarm to green but not re-enable the host encryption mode now.
   When you click either **Acknowledge** or **Reset to green**, the alarm goes way, but the host's encryption mode remains disabled until you re-enable it.
4. Navigate to the ESXi host's **Monitor** tab and click **Events** to get more information on why encryption mode is disabled.
   Perform suggested troubleshooting before you re-enable the encryption mode.
5. On the **Summary** tab, click **Enable Host Encryption Mode** to re-enable host encryption.
   A message appears, warning that encryption key data is transmitted to the host.
6. Click **Yes**.

Set Key Management Server Certificate Expiration Threshold

By default, vCenter Server notifies you 30 days before your Key Management Server (KMS) certificates expire. You can change this default value.

KMS certificates have an expiration date. When the threshold for the expiration date is reached, an alarm notifies you.

vCenter Server and key providers exchange two types of certificates: server and client. The VMware Endpoint Certificate Store (VECS) on the vCenter Server system stores the server certificates and one client certificate per key provider. Because there are two certificate types, there are two alarms for each certificate type (one for client, one for server).

1. Log in to a vCenter Server system by using the vSphere Client.
2. Select the vCenter Server system in the object hierarchy.
3. Click **Configure**.
4. Under **Settings**, click **Advanced Settings**, and click **Edit Settings**.
5. Click the **Filter** icon and enter `vpxd.kmscert.threshold` , or scroll to the configuration parameter itself.
6. Enter your value in days and click **Save**.

vSphere Virtual Machine Encryption and Core Dumps

If your environment uses vSphere Virtual Machine Encryption, and if an error occurs on the ESXi host, the resulting core dump is encrypted to protect customer data. Core dumps that are included in the vm-support package are also encrypted.

Note: Core dumps can contain sensitive information. Follow your organization's data security and privacy policy when handling core dumps.

Core Dumps on ESXi Hosts

When an ESXi host, a user world, or a virtual machine fails, a core dump is generated, and the host reboots. If the ESXi host has encryption mode enabled, the core dump is encrypted using a key that is in the ESXi key cache. This key comes from the KMS. See How vSphere Virtual Machine Encryption Protects Your Environment for background information.

When an ESXi host is cryptographically "safe," and a core dump is generated, an event is created. The event indicates that a core dump occurred along with the following information: world name, occurring times, keyID of the key used to

encrypt the core dump, and core dump filename. You can view the event in the Events viewer under **Tasks and Events** for the vCenter Server.

The following table shows encryption keys used for each core dump type, by vSphere release.

Table 266: Core Dump Encryption Keys

Core Dump Type	Encryption Key (ESXi 6.5)	Encryption Key (ESXi 6.7 and Later)
ESXi Kernel	Host Key	Host Key
User World (hostd)	Host Key	Host Key
Encrypted Virtual Machine (VM)	Host Key	Virtual Machine Key

What you can do after an ESXi host reboot depends on several factors.

- In most cases, vCenter Server retrieves the key for the host from the KMS and attempts to push the key to the ESXi host after reboot. If the operation is successful, you can generate the vm-support package and you can decrypt or re-encrypt the core dump. See Decrypt or Re-Encrypt an Encrypted Core Dump.
- If vCenter Server cannot connect to the ESXi host, you might be able to retrieve the key from the KMS. See Resolve Missing Key Issues.
- If the host used a custom key, and that key differs from the key that vCenter Server pushes to the host, you cannot manipulate the core dump. Avoid using custom keys.

Core Dumps and vm-support Packages

When you contact VMware Technical Support because of a serious error, your support representative usually asks you to generate a vm-support package. The package includes log files and other information, including core dumps. If your support representatives cannot resolve the issues by looking at log files and other information, they might ask you to decrypt the core dumps and make relevant information available. To protect sensitive information such as keys, follow your organization's security and privacy policy. See Collect a vm-support Package for an ESXi Host That Uses Encryption.

Core Dumps on vCenter Server Systems

A core dump on a vCenter Server system is not encrypted. vCenter Server already contains potentially sensitive information. At the minimum, ensure that the vCenter Server is protected. See Securing vCenter Server Systems. You might also consider turning off core dumps for the vCenter Server system. Other information in log files can help determine the problem.

Collect a vm-support Package for an ESXi Host That Uses Encryption

If host encryption mode is enabled for the ESXi host, any core dumps in the `vm-support` package are encrypted. You can collect the package from the vSphere Client, and you can specify a password if you expect to decrypt the core dump later.

Inform your support representative that host encryption mode is enabled for the ESXi host. Your support representative might ask you to decrypt core dumps and extract relevant information.

Note: Core dumps can contain sensitive information. Follow your organization's security and privacy policy to protect sensitive information such as host keys.

The `vm-support` package includes log files, core dump files, and more.

1. Log in to the vCenter Server system with the vSphere Client.
2. Click **Hosts & Clusters**, and right-click the ESXi host.
3. Select **Export System Logs**.
4. In the dialog box, select **Password for encrypted core dumps**, and specify and confirm a password.
5. Leave the defaults for other options or make changes if requested by VMware Technical Support, and click **Export Logs**.

   If you have not configured your browser to ask where to save files before downloading, the download starts. If you have configured your browser to ask where to save files, specify a location for the file.
6. If your support representative asked you to decrypt the core dump in the `vm-support` package, log in to any ESXi host and follow these steps.
   a) Log in to the ESXi host and connect to the directory where the `vm-support` package is located.

      The filename follows the pattern esx.date_and_time.tgz.
   b) Make sure that the directory has enough space for the package, the uncompressed package, and the recompressed package, or move the package.
   c) Extract the package to the local directory.

      ```
      vm-support -x *.tgz .
      ```

      The resulting file hierarchy might contain core dump files for the ESXi host, usually in `/var/core`, and might contain multiple core dump files for virtual machines.
   d) Decrypt each encrypted core dump file separately.

      ```
      crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
      --password encryptedZdumpdecryptedZdump
      ```

      `vm-support-incident-key-file` is the incident key file that you find at the top level in the directory.

      `encryptedZdump` is the name of the encrypted core dump file.

      `decryptedZdump` is the name for the file that the command generates. Make the name similar to the *`encryptedZdump`* name.
   e) Provide the password that you specified when you created the `vm-support` package.
   f) Remove the encrypted core dumps, and compress the package again.

      ```
      vm-support --reconstruct
      ```
7. Remove any files that contain confidential information.

Decrypt or Re-Encrypt an Encrypted Core Dump

You can decrypt or re-encrypt an encrypted core dump on your ESXi host by using the `crypto-util` CLI.

The key that was used to encrypt the core dump must be available on the ESXi host that generated the core dump.

You can decrypt and examine the core dumps in the vm-support package yourself. Core dumps might contain sensitive information. Follow your organization's security and privacy policy to protect sensitive information such as keys.

For details about re-encrypting a core dump and other features of `crypto-util`, see the command-line help.

Note: `crypto-util` is for advanced users.

1. Log directly in to the ESXi host on which the core dump happened.
   If the ESXi host is in lockdown mode, or if SSH access is disabled, you might have to enable access first.
2. Determine whether the core dump is encrypted.

Option	Description
Monitor core dump	`crypto-util envelope describe vmmcores.ve`
zdump file	`crypto-util envelope describe --offset 4096 zdump-File`

3. Decrypt the core dump, depending on its type.

Option	Description
Monitor core dump	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump file	`crypto-util envelope extract --offset 4096 zdumpEn-cryptedzdumpUnencrypted`

Enable and Disable Key Persistence on an ESXi Host

You must enable key persistence on an ESXi host. It is not enabled by default.

Requirements to enable key persistence:

- ESXi 7.0 Update 2 or later
- ESXi host installed with TPM 2.0
- Have access to the ESXCLI command set. You can run ESXCLI commands remotely, or run them in the ESXi Shell.

Note: Key persistence is not necessary when using vSphere Native Key Provider. vSphere Native Key Provider is designed out-of-the-box to run without requiring access to a key server.

For additional security, the TPM can also use a sealing policy to prevent tampering during ESXi host boot. See TPM Sealing Policies Overview.

For conceptual information about key persistence, see Key Persistence Overview.

1. Start a session on the ESXi host by using SSH or another remote console connection.
2. Log in as root.
3. Verify that the ESXi host is in TPM mode.

   ```
   esxcli system settings encryption get
   ```

   If the Mode appears as NONE, you must enable the TPM in the firmware of the host, and set the mode by running the following command.

   ```
   esxcli system settings encryption set --mode=TPM
   ```

4. Enable or disable key persistence.
   a) To enable key persistence:

      ```
      esxcli system security keypersistence enable
      ```

   b) To disable persistence:

      ```
      esxcli system security keypersistence disable --remove-all-stored-keys
      ```

Rekey an Encrypted Virtual Machine Using the vSphere Client

You can use the vSphere Client to perform a shallow rekey of an encrypted virtual machine. You might perform a rekey of an encrypted virtual machine for business or compliance reasons.

Required privilege: **Cryptographic operations** > **Manage key servers**

A shallow rekey, or rekey (also called a shallow recrypt), enables you to use a new (and different) Key Encryption Key (KEK) on an encrypted virtual machine. You can perform a rekey operation while the virtual machine is powered on. You can also perform a rekey if the virtual machine has snapshots present. Rekeying of an encrypted virtual machine with snapshots is permitted only on a single snapshot branch (disk chain). Multiple snapshot branches are not supported. If the rekey fails before updating all links in the chain with the new KEK, you can still access the encrypted virtual machine if you have the old and new KEKs.

1. Log in to the vCenter Server system with the vSphere Client.
2. Browse the inventory list and select the encrypted virtual machine.
3. Right-click the encrypted virtual machine and select **VM Policies**.
4. Select **Re-encrypt**.
5. Click **Yes**.

   The encrypted virtual machine is rekeyed with the new KEK.

   Note: If the rekey fails, the events subsystem posts the following event:

   `com.vmware.vc.vm.crypto.RekeyFail`

Securing Virtual Machines with Virtual Trusted Platform Module

With the Virtual Trusted Platform Module (vTPM) feature, you can add a TPM 2.0 virtual cryptoprocessor to a virtual machine.

A vTPM is a software-based representation of a physical Trusted Platform Module 2.0 chip. A vTPM acts as any other virtual device. You can add a vTPM to a virtual machine in the same way you add virtual CPUs, memory, disk controllers, or network controllers. A vTPM does not require a hardware Trusted Platform Module chip.

Virtual Trusted Platform Module Overview

A virtual Trusted Platform Module (vTPM) is a software-based representation of a physical Trusted Platform Module 2.0 chip. A vTPM acts as any other virtual device.

What Is a vTPM

vTPMs provide hardware-based, security-related functions such as random number generation, attestation, key generation, and more. When added to a virtual machine, a vTPM enables the guest operating system to create and store keys that are private. These keys are not exposed to the guest operating system itself. Therefore, the virtual machine attack surface is reduced. Usually, compromising the guest operating system compromises its secrets, but enabling a vTPM greatly reduces this risk. These keys can be used only by the guest operating system for encryption or signing. With an attached vTPM, a client can remotely attest the identity of the virtual machine, and verify the software that it is running.

You can add a vTPM to either a new or an existing virtual machine. A vTPM depends on virtual machine encryption to secure vital TPM data. When you configure a vTPM, the virtual machine files are encrypted but not the disks. You can choose to add encryption explicitly for the virtual machine and its disks.

When you back up a virtual machine enabled with a vTPM, the backup must include all virtual machine data, including the `*.nvram` file. If your backup does not include the `*.nvram` file, you cannot restore a virtual machine with a vTPM. Also, because the VM home files of a vTPM-enabled virtual machine are encrypted, ensure that the encryption keys are available at the time of a restore.

Note: By default, no storage policy is associated with a virtual machine that has been enabled with a vTPM. Only the virtual machine files (VM Home) are encrypted. If you prefer, you can choose to add encryption explicitly for the virtual machine and its disks, but the virtual machine files would have already been encrypted.

vSphere Requirements for vTPMs

To use a vTPM, your vSphere environment must meet these requirements:

- Virtual machine requirements:
  - EFI firmware
  - Hardware version 14 and later
- Component requirements:
  - vCenter Server 6.7 and later for Windows virtual machines, vCenter Server 7.0 Update 2 and later for Linux virtual machines.
  - Virtual machine encryption (to encrypt the virtual machine home files).
- Guest OS support:
  - Linux
  - Windows Server 2008 and later
  - Windows 7 and later

Differences between a Hardware TPM and a Virtual TPM

You use a hardware Trusted Platform Module (TPM) to provide secure storage of credentials or keys. A vTPM performs the same functions as a TPM, but it performs cryptographic coprocessor capabilities in software. A vTPM uses the `.nvram` file, which is encrypted using virtual machine encryption, as its secure storage.

A hardware TPM includes a preloaded key called the Endorsement Key (EK). The EK has a private and public key. The EK provides the TPM with a unique identity. For a vTPM, this key is provided either by the VMware Certificate Authority (VMCA) or by a third-party Certificate Authority (CA). After the vTPM uses a key, it is typically not changed because doing so invalidates sensitive information stored in the vTPM. The vTPM does not contact the third-party CA at any time.

Create a Virtual Machine with a Virtual Trusted Platform Module

You can add a Virtual Trusted Platform Module (vTPM) when you create a virtual machine to provide enhanced security to the guest operating system. You must create a key provider before you can add a vTPM.

- The guest OS you use can be Windows Server 2008 and later, Windows 7 and later, or Linux.
- The ESXi hosts running in your environment must be ESXi 6.7 or later (Windows guest OS), or 7.0 Update 2 (Linux guest OS).
- The virtual machine must use EFI firmware.
- Verify that you have the required privileges:
  - **Cryptographic operations** > **Clone**
  - **Cryptographic operations** > **Encrypt**
  - **Cryptographic operations** > **Encrypt new**
  - **Cryptographic operations** > **Migrate**
  - **Cryptographic operations** > **Register VM**

Note: After creating a virtual machine with a vTPM, the**Cryptographic operations** > **Direct Access** privilege is required to open a console session.

The VMware virtual TPM is compatible with TPM 2.0 and creates a TPM-enabled virtual chip for use by the virtual machine and the guest OS it hosts.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object, select **New Virtual Machine**, and follow the prompts to create a virtual machine.

Option	Action
Select a creation type	Create a new virtual machine.
Select a name and folder	Specify a name and target location.
Select a compute resource	
Select storage	Select a compatible datastore.
Select compatibility	You must select **ESXi 6.7 and later** for Windows guest OS, or **ESXi 7.0 U2** and later for Linux guest OS.
Select a guest OS	Select Windows or Linux for use as the guest OS.
Customize hardware	Click **Add New Device** and select **Trusted Platform Module**. You can further customize the hardware, for example, by changing disk size or CPU.
Ready to complete	Review the information and click **Finish**.

The vTPM-enabled virtual machine appears in your inventory as specified.

Enable Virtual Trusted Platform Module for an Existing Virtual Machine

You can add a Virtual Trusted Platform Module (vTPM) to an existing virtual machine to provide enhanced security to the guest operating system. You must create a key provider before you can add a vTPM.

- The guest OS you use can be Windows Server 2008 and later, Windows 7 and later, or Linux.
- Verify that the virtual machine is turned off.
- The ESXi hosts running in your environment must be ESXi 6.7 or later (Windows guest OS), or 7.0 Update 2 (Linux guest OS).
- The virtual machine must use EFI firmware.
- Verify that you have the required privileges:
  - **Cryptographic operations** > **Clone**
  - **Cryptographic operations** > **Encrypt**
  - **Cryptographic operations** > **Encrypt new**
  - **Cryptographic operations** > **Migrate**
  - **Cryptographic operations** > **Register VM**
  - **Virtual machine** > **Configuration** > **Add or remove device**

Note: After adding a vTPM to a virtual machine, the **Cryptographic operations** > **Direct Access** privilege is required to open a console session.

The VMware virtual TPM is compatible with TPM 2.0, and creates a TPM-enabled virtual chip for use by the virtual machine and the guest OS it hosts.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, click **Add New Device** and select **Trusted Platform Module**.
4. Click **OK**.

   The virtual machine **Summary** tab now includes Virtual Trusted Platform Module in the **VM Hardware** pane.

Remove Virtual Trusted Platform Module from a Virtual Machine

You can remove Virtual Trusted Platform Module (vTPM) security from a virtual machine.

- Ensure that the virtual machine is powered off.
- Verify that you have the required privilege: **Cryptographic operations** > **Decrypt**

Removing a vTPM device causes all encrypted information on the virtual machine to become unrecoverable. Before removing a vTPM from a virtual machine, deactivate any applications in the Guest OS that use the vTPM device, such as BitLocker. Failure to do so can cause the virtual machine not to boot. Also, you cannot remove a vTPM from a virtual machine that contains snapshots.

1. Connect to vCenter Server by using the vSphere Client.
2. Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
3. In the **Edit Settings** dialog box, locate the Trusted Platform Module entry in the **Virtual Hardware** tab.
4. Move your pointer over the device and click the **Remove** icon.

   This icon appears only for the virtual hardware that you can safely remove.
5. Click **Delete** to confirm you want to remove the device.

   The vTPM device is marked for removal.
6. Click **OK**.

   Verify that the Virtual Trusted Platform Module entry no longer appears in the virtual machine **Summary** tab in the **VM Hardware** pane.

Identify Virtual Trusted Platform Module Enabled Virtual Machines

You can identify which of your virtual machines are enabled to use a Virtual Trusted Platform Module (vTPM).

You can generate a list of all virtual machines in your inventory showing virtual machine name, operating system, and vTPM status. You can also export this list to a CSV file for use in compliance audits.

1. Connect to vCenter Server by using the vSphere Client.
2. Select a vCenter Server instance, a host, or a cluster.
3. Click the **VMs** tab and click **Virtual Machines**.
4. To view all virtual machines on which a TPM is enabled, click the three-bar **Column Selector** in the lower left corner and select **TPM**.

   The TPM column displays "Present" for virtual machines on which a TPM is enabled. Virtual machines without a TPM are listed as "Not present."

5. You can export the contents of an inventory list view to a CSV file.
   a) Click **Export** at the bottom-right corner of a list view.
      The Export List Contents dialog box opens and lists the available options for inclusion in the CSV file.
   b) Select whether you want all rows or your current selection of rows to be listed in the CSV file.
   c) From the available options, select the columns you want listed in the CSV file.
   d) Click **Export**.
      The CSV file is generated and available for download.

View Virtual Trusted Platform Module Device Certificates

Virtual Trusted Platform Module (vTPM) devices are pre-configured with default certificates, which you can review.

You must have a vTPM-enabled virtual machine in your environment.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Click **VMs** and click **Virtual Machines**.
4. Select the vTPM-enabled virtual machine whose certificate information you want to view.
   If necessary, click the three-bar **Column Selector** in the lower left corner and select **TPM** to display virtual machines with a TPM "Present."
5. Click the **Configure** tab.
6. Under **TPM**, select **Certificates**.
7. Select the certificate and view its information.
8. (Optional) To export the certificate information, click **Export**.
   The certificate is saved to disk.

You can replace the default certificate with a certificate issued by a third-party certificate authority (CA). See Export and Replace Virtual Trusted Platform Module Device Certificates.

Export and Replace Virtual Trusted Platform Module Device Certificates

You can replace the default certificate that comes with a Virtual Trusted Platform Module (vTPM) device.

You must have a vTPM-enabled virtual machine in your environment.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Select the vTPM-enabled virtual machine in the inventory whose certificate information you want to replace.
4. Click the **Configure** tab.
5. Under **TPM** select **Signing Requests**.
6. Select a certificate.
7. To export the certificate information, click **Export**.
   The certificate is saved to disk.

8. Get a certificate issued by a third-party certificate authority (CA) against the certificate signing request (CSR) you exported.

   You can use any CA that you might have in your IT environment.

9. When you have the new certificate, replace the existing certificate.
   a) Right-click the virtual machine in the inventory whose certificate you want to replace and select **Edit Settings**.
   b) In the **Edit Settings** dialog box, expand **Security Devices**, then expand **Trusted Platform Module**.

      The certificates appear.
   c) Click **Replace** for the certificate you want to replace.

      The **File Upload** dialog box appears.
   d) On your local machine, locate the new certificate and upload it.

      The new certificate replaces the default certificate that came with your vTPM device.
   e) The certificate name is updated in the virtual machine **Summary** tab under the **Virtual Trusted Platform Module** list.

Securing Windows Guest Operating Systems with Virtualization-based Security

Starting with vSphere 6.7, you can enable Microsoft virtualization-based security (VBS) on supported Windows guest operating systems.

Microsoft VBS, a feature of Windows 10 and Windows Server 2016 operating systems, uses hardware and software virtualization to enhance system security by creating an isolated, hypervisor-restricted, specialized subsystem.

VBS permits you to use the following Windows security features to harden your system and isolate key system and user secrets from being compromised:

- Credential Guard: Aims to isolate and harden key system and user secrets against compromise.
- Device Guard: Provides a set of features designed to work together to prevent and eliminate malware from running on a Windows system.
- Configurable Code Integrity: Ensures that only trusted code runs from the boot loader onwards.

See the topic on virtualization-based security in the Microsoft documentation for more information.

After you enable VBS for a virtual machine through vCenter Server, you enable VBS within the Windows guest operating system.

Virtualization-based Security Best Practices

Follow best practices for virtualization-based security (VBS) to maximize security and manageability of your Windows guest operating system environment.

Avoid problems by following these best practices.

VBS Hardware

Use the following hardware for VBS:

- Intel
  - Haswell CPU or later. For best performance, use the Skylake-EP CPU or later.
  - The Ivy Bridge CPU is acceptable.
  - The Sandy Bridge CPU might cause some slow performance.

- AMD
  - Zen 2 series CPUs (Rome) or later.
  - Older CPUs might cause some slow performance.

The mitigations for the Machine Check Exception on Page Size Change Intel CPU vulnerability can impact guest OS performance negatively when VBS is in use. For more information, see the VMware KB article at https://kb.vmware.com/kb/76050.

Windows Guest OS Compatibility

On Intel, VBS is supported for Windows 10 and Windows Server 2016 and later virtual machines, although Windows Server 2016 versions 1607 and 1703 require patches. Check the Microsoft documentation for ESXi host hardware compatibility. Using Intel CPUs for VBS requires vSphere 6.7 or later and hardware version 14.

On AMD, VBS is supported on Windows 10, version 1809, and Windows 2019 and later virtual machines. Using AMD CPUs for VBS requires vSphere 7.0 Update 2 or later and hardware version 19.

Initially, Windows 10 required that you enable Hyper-V for VBS. Enabling Hyper-V is not required for Windows 10. The same applies to Windows Server 2016 and later. Consult the current Microsoft documentation and the *VMware vSphere Release Notes* for more information.

Unsupported VMware Features on VBS

The following features are not supported in a virtual machine when VBS is enabled:

- Fault tolerance
- PCI passthrough
- Hot add of CPU or memory

Installation and Upgrade Caveats with VBS

Before you configure VBS, understand the following installation and upgrade caveats:

- New virtual machines configured for Windows 10 and Windows Server 2016 and later on virtual hardware versions less than version 14 are created using Legacy BIOS by default. You must reinstall the guest operating system after changing the virtual machine's firmware type from Legacy BIOS to UEFI.
- If you plan to migrate your virtual machines from previous vSphere releases to vSphere 6.7 or greater, and enable VBS on your virtual machines, use UEFI to avoid having to reinstall the operating system.

Enable Virtualization-based Security on a Virtual Machine

You can enable Microsoft virtualization-based security (VBS) for supported Windows guest operating systems at the same time you create a virtual machine.

See Virtualization-based Security Best Practices for acceptable CPUs.

Using Intel CPUs for VBS requires vSphere 6.7 or later. Create a virtual machine that uses hardware version 14 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit) or later releases
- Windows Server 2016 (64 bit) or later releases

Using AMD CPUs for VBS requires vSphere 7.0 Update 2 or later. Create a virtual machine that uses hardware version 19 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit), version 1809 or later releases
- Windows Server 2019 (64 bit) or later releases

Ensure that you install the latest patches for Windows 10, version 1809, and Windows Server 2019, before enabling VBS.

For more information about activating VBS on virtual machines on AMD platforms, see the VMware KB article at https://kb.vmware.com/s/article/89880.

Enabling VBS is a process that involves first enabling VBS in the virtual machine then enabling VBS in the Windows guest OS.

1. Connect to vCenter Server by using the vSphere Client.
2. Select an object in the inventory that is a valid parent object of a virtual machine, for example, an ESXi host or a cluster.
3. Right-click the object, select **New Virtual Machine**, and follow the prompts to create a virtual machine.

Option	Action
Select a creation type	Create a virtual machine.
Select a name and folder	Specify a name and target location.
Select a compute resource	Specify an object for which you have privileges to create virtual machines.
Select storage	In the VM storage policy, select the storage policy. Select a compatible datastore.
Select compatibility	Intel CPU: Ensure that **ESXi 6.7 and later** is selected. AMD CPU: Ensure that **ESXi 7.0 U2 and later** is selected.
Select a guest OS	Select the Windows guest operating system option that best corresponds to operating system release. Select the **Enable Windows Virtualization Based Security** check box.
Customize hardware	Customize the hardware, for example, by changing disk size or CPU.
Ready to complete	Review the information and click **Finish**.

Once the virtual machine is created, confirm that its **Summary** tab displays "VBS true" in the Guest OS description.

See Enable Virtualization-based Security on the Guest Operating System.

Enable Virtualization-based Security on an Existing Virtual Machine

You can enable Microsoft virtualization-based security (VBS) on existing virtual machines for supported Windows guest operating systems.

Using Intel CPUs for VBS requires vSphere 6.7 or later. The virtual machine must have been created using hardware version 14 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit) or later releases
- Windows Server 2016 (64 bit) or later releases

Using AMD CPUs for VBS requires vSphere 7.0 Update 2 or later. The virtual machine must have been created using hardware version 19 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit), version 1809 or later releases
- Windows Server 2019 (64 bit) or later releases

Ensure that you install the latest patches for Windows 10, version 1809, and Windows Server 2019, before enabling VBS.

For more information about activating VBS on virtual machines on AMD platforms, see the VMware KB article at https://kb.vmware.com/s/article/89880.

Enabling VBS is a process that involves first enabling VBS in the virtual machine then enabling VBS in the guest OS.

Note: New virtual machines configured for Windows 10, Windows Server 2016, and Windows Server 2019 on hardware versions less than version 14 are created using Legacy BIOS by default. If you change the virtual machine's firmware type from Legacy BIOS to UEFI, you must reinstall the guest operating system.

1. In the vSphere Client, browse to the virtual machine.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click the **VM Options** tab.
4. Select the **Enable** check box for Virtualization Based Security.
5. Click **OK**.

Confirm that the virtual machine's **Summary** tab displays "VBS true" in the Guest OS description.

See Enable Virtualization-based Security on the Guest Operating System.

Enable Virtualization-based Security on the Guest Operating System

You can enable Microsoft virtualization-based security (VBS) for supported Windows guest operating systems.

- Ensure that virtualization-based security has been enabled on the virtual machine.

You enable VBS from within the Windows Guest OS. Windows configures and enforces VBS through a Group Policy Object (GPO). The GPO gives you the ability to turn off and on the various services, such as Secure Boot, Device Guard, and Credential Guard, that VBS offers. Certain Windows versions also require you to perform the additional step of enabling the Hyper-V platform.

See Microsoft's documentation about deploying Device Guard to enable virtualization-based security for details.

1. In Microsoft Windows, edit the group policy to turn on VBS and choose other VBS-related security options.
2. Optional: For Microsoft Windows versions less than Redstone 4, in the Windows Features control panel, enable the Hyper-V platform.
3. Reboot the guest operating system.

Deactivate Virtualization-based Security

If you no longer use virtualization-based security (VBS) with a virtual machine, you can deactivate VBS. When you deactivate VBS for the virtual machine, the Windows VBS options remain unchanged but might induce performance issues. Before deactivating VBS on the virtual machine, deactivate VBS options within Windows.

Ensure that the virtual machine is powered off.

1. In the vSphere Client, browse to the virtual machine that is using VBS.
   See Identify VBS-Enabled Virtual Machines for help in locating virtual machines that use VBS.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click **VM Options**.
4. Deselect the **Enable** check box for Virtualization Based Security.
   A message reminds you to deactivate VBS in the guest OS.

5. Click **OK**.
6. Verify that the virtual machine's **Summary** tab no longer displays "VBS true" in the Guest OS description.

Identify VBS-Enabled Virtual Machines

You can identify which of your virtual machines have VBS enabled, for reporting and compliance purposes.

1. Connect to vCenter Server by using the vSphere Client.
2. Select a vCenter Server instance, a data center, or a host in the inventory.
3. Click the **VMs** tab and click **Virtual Machines**.
4. In the list of virtual machines, click the down arrow in a column header to show/hide columns, and select the **VBS** check box.

   The **VBS** column appears.
5. Scan for Present in the **VBS** column.

Securing vSphere Networking

Securing vSphere Networking is an essential part of protecting your environment. You secure different vSphere components in different ways. See the *vSphere Networking* documentation for detailed information about networking in the vSphere environment.

Introduction to vSphere Network Security

Network security in the vSphere environment shares many characteristics of securing a physical network environment, but also includes some characteristics that apply only to virtual machines.

Firewalls

Add firewall protection to your virtual network by installing and configuring host-based firewalls on some or all its VMs.

For efficiency, you can set up private virtual machine Ethernet networks or virtual networks. With virtual networks, you install a host-based firewall on a VM at the head of the virtual network. This firewall serves as a protective buffer between the physical network adapter and the remaining VMs in the virtual network.

Host-based firewalls can slow performance. Balance your security needs against performance goals before you install host-based firewalls on VMs elsewhere in the virtual network.

See Securing the Network with Firewalls.

Segmentation

Keep different virtual machine zones within a host on different network segments. If you isolate each virtual machine zone on its own network segment, you minimize the risk of data leakage from one zone to the next. Segmentation prevents various threats, including Address Resolution Protocol (ARP) spoofing. With ARP spoofing, an attacker manipulates the ARP table to remap MAC and IP addresses, and gains access to network traffic to and from a host. Attackers use ARP spoofing to generate man in the middle (MITM) attacks, perform denial of service (DoS) attacks, hijack the target system, and otherwise disrupt the virtual network.

Planning segmentation carefully lowers the chances of packet transmissions between virtual machine zones. Segmentation therefore prevents sniffing attacks that require sending network traffic to the victim. Also, an attacker cannot use a nonsecure service in one virtual machine zone to access other virtual machine zones in the host. You can implement segmentation by using one of two approaches.

- Use separate physical network adapters for virtual machine zones to ensure that the zones are isolated. Maintaining separate physical network adapters for virtual machine zones is probably the most secure method. After the initial segment creation. This approach is less prone to misconfiguration.
- Set up virtual local area networks (VLANs) to help safeguard your network. VLANs provide almost all the security benefits inherent in implementing physically separate networks without the hardware overhead. VLANs can save you the cost of deploying and maintaining additional devices, cabling, and so on. See Securing Virtual Machines with VLANs.

Preventing Unauthorized Access

Requirements for securing VMs are often the same as requirements for securing physical machines.

- If a virtual machine network is connected to a physical network, it can be subject to breaches just like a network that consists of physical machines.
- Even if you do not connect a VM to the physical network, the VM can be attacked by other VMs.

VMs are isolated from each other. One VM cannot read or write another VM's memory, access its data, use its applications, and so forth. However, within the network, any VM or group of VMs can still be the target of unauthorized access from other VMs. Protect your VMs from such unauthorized access.

For additional information about protecting VMs, see the NIST document titled " Secure Virtual Network Configuration for Virtual Machine (VM) Protection" at:

https://csrc.nist.gov/publications/detail/sp/800-125b/final

Securing the Network with Firewalls

Security administrators use firewalls to safeguard the network or selected components in the network from intrusion.

Firewalls control access to devices within their perimeter by closing all ports except for ports that the administrator explicitly or implicitly designates as authorized. The ports that administrators open allow traffic between devices on different sides of the firewall.

Important: The ESXi firewall in ESXi 5.5 and later does not allow per-network filtering of vMotion traffic. Therefore, you must install rules on your external firewall to ensure that no incoming connections can be made to the vMotion socket.

In a virtual machine environment, you can plan the layout for firewalls between components.

- Firewalls between physical machines such as vCenter Server systems and ESXi hosts.
- Firewalls between one virtual machine and another, for example, between a virtual machine acting as an external Web server and a virtual machine connected to your company's internal network.
- Firewalls between a physical machine and a virtual machine, such as when you place a firewall between a physical network adapter card and a virtual machine.

How you use firewalls in your ESXi configuration is based on how you plan to use the network and how secure any given component has to be. For example, if you create a virtual network where each virtual machine is dedicated to running a different benchmark test suite for the same department, the risk of unwanted access from one virtual machine to the next is minimal. Therefore, a configuration where firewalls are present between the virtual machines is not necessary. However, to prevent interruption of a test run from an outside host, you can configure a firewall at the entry point of the virtual network to protect the entire set of virtual machines.

For the list of all supported ports and protocols in VMware products, including vSphere and vSAN, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/. You can search ports by VMware product, create a customized list of ports, and print or save port lists.

Firewalls for Configurations with vCenter Server

If you access ESXi hosts through vCenter Server, you typically protect vCenter Server using a firewall.

Firewalls must be present at entry points. A firewall might lie between the clients and vCenter Server or vCenter Server and the clients can both be behind a firewall.

For the list of all supported ports and protocols in VMware products, including vSphere and vSAN, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/. You can search ports by VMware product, create a customized list of ports, and print or save port lists.

Networks configured with vCenter Server can receive communications through the vSphere Client, other UI clients, or clients that use the vSphere API. During normal operation, vCenter Server listens for data from its managed hosts and clients on designated ports. vCenter Server also assumes that its managed hosts listen for data from vCenter Server on designated ports. If a firewall is present between any of these elements, you must ensure that the firewall has open ports to support data transfer.

You might also include firewalls at other access points in the network, depending on the network usage and on the level of security that clients require. Select the locations for your firewalls based on the security risks for your network configuration. The following firewall locations are commonly used.

- Between the vSphere Client or a third-party network-management client and vCenter Server.
- If your users access virtual machines through a Web browser, between the Web browser and the ESXi host.
- If your users access virtual machines through the vSphere Client, between the vSphere Client and the ESXi host. This connection is in addition to the connection between the vSphere Client and vCenter Server, and it requires a different port.
- Between vCenter Server and the ESXi hosts.
- Between the ESXi hosts in your network. Although traffic between hosts is usually considered trusted, you can add firewalls between them if you are concerned about security breaches from machine to machine.

  If you add firewalls between ESXi hosts and plan to migrate virtual machines between them, open ports in any firewall that divides the source host from the target hosts.
- Between the ESXi hosts and network storage such as NFS or iSCSI storage. These ports are not specific to VMware. Configure them according to the specifications for your network.

Connecting to vCenter Server Through a Firewall

Open TCP port 443 in the firewall to enable vCenter Server to receive data.

By default vCenter Server uses TCP port 443 to listen for data from its clients. If you have a firewall between vCenter Server and its clients, you must configure a connection through which vCenter Server can receive data from the clients. Firewall configuration depends on what is used at your site, ask your local firewall system administrator for information.

Connecting ESXi Hosts Through Firewalls

If you have a firewall between your ESXi hosts and vCenter Server, ensure that the managed hosts can receive data.

To configure a connection for receiving data, open ports for traffic from services such as vSphere High Availability, vMotion, and vSphere Fault Tolerance. See ESXi Firewall Configuration for a discussion of configuration files, vSphere Client access, and firewall commands. For a list of ports, see the VMware Ports and Protocols Tool™ at https://ports.broadcom.com/.

Firewalls for Configurations Without vCenter Server

If your environment does not include vCenter Server, clients can connect directly to the ESXi network.

You can connect to a standalone ESXi host in several ways.

- VMware Host Client
- ESXCLI interface
- vSphere Web Services SDK or vSphere Automation SDKs
- Third-party clients

The firewall requirements for standalone hosts are similar to requirements when a vCenter Server is present.

- Use a firewall to protect your ESXi layer or, depending on your configuration, your clients, and the ESXi layer. This firewall provides basic protection for your network.
- Licensing in this type of configuration is part of the ESXi package that you install on each of the hosts. Because licensing is resident to ESXi, a separate License Server with a firewall is not required.

You can configure firewall ports using ESXCLI or using the VMware Host Client. See *vSphere Single Host Management - VMware Host Client*.

Connecting to the Virtual Machine Console Through a Firewall

Certain ports must be open for user and administrator communication with the virtual machine console. Which ports must be open depends on the type of virtual machine console, and on whether you connect through vCenter Server with the vSphere Client or directly to the ESXi host from the VMware Host Client.

For more information about ports, purpose, and classification (incoming, outgoing, or bidirectional), see the VMware Ports and Protocols Tool™ at https://ports.vmware.com.

Connecting to a Browser-Based Virtual Machine Console Through the vSphere Client

When you are connecting with the vSphere Client, you always connect to the vCenter Server system that manages the ESXi host, and access the virtual machine console from there.

If you are using the vSphere Client and connecting to a browser-based virtual machine console, the following access must be possible:

- The firewall must allow vSphere Client to access vCenter Server on port 443.
- The firewall must allow vCenter Server to access the ESXi host on port 902.

Connecting to a VMware Remote Console Through the vSphere Client

If you are using the vSphere Client and connecting to a VMware Remote Console (VMRC), the following access must be possible:

- The firewall must allow the vSphere Client to access vCenter Server on port 443.
- The firewall must allow the VMRC to access vCenter Server on port 443 and to access the ESXi host on port 902 for VMRC versions before 11.0, and port 443 for VMRC version 11.0 and greater. For more information about VMRC version 11.0 and ESXi port requirements, see the VMware knowledge base article at https://kb.vmware.com/s/article/76672.

Connecting to ESXi Hosts Directly with the VMware Host Client

You can use the VMware Host Client virtual machine console if you connect directly to an ESXi host.

Note: Do not use the VMware Host Client to connect directly to hosts that are managed by a vCenter Server system. If you make changes to such hosts from the VMware Host Client, instability in your environment results.

The firewall must allow access to the ESXi host on ports 443 and 902.

The VMware Host Client uses port 902 to provide a connection for guest operating system MKS activities on virtual machines. It is through this port that users interact with the guest operating systems and applications of the virtual machine. VMware does not support configuring a different port for this function.

Secure the Physical Switch

Secure the physical switch on each ESXi host to prevent attackers from gaining access to the host and its virtual machines.

For best protection of your hosts, ensure that physical switch ports are configured with spanning tree disabled and ensure that the non-negotiate option is configured for trunk links between external physical switches and virtual switches in Virtual Switch Tagging (VST) mode.

1. Log in to the physical switch and ensure that spanning tree protocol is disabled or that Port Fast is configured for all physical switch ports that are connected to ESXi hosts.
2. For virtual machines that perform bridging or routing, check periodically that the first upstream physical switch port is configured with BPDU Guard and Port Fast disabled and with spanning tree protocol enabled.

   In vSphere 5.1 and later, to prevent the physical switch from potential Denial of Service (DoS) attacks, you can turn on the guest BPDU filter on the ESXi hosts.
3. Log in to the physical switch and ensure that Dynamic Trunking Protocol (DTP) is not enabled on the physical switch ports that are connected to the ESXi hosts.
4. Routinely check physical switch ports to ensure that they are properly configured as trunk ports if connected to virtual switch VLAN trunking ports.

Securing Standard Switch Ports with Security Policies

The VMkernel port group or virtual machine port group on a standard switch has a configurable security policy. The security policy determines how strongly you enforce protection against impersonation and interception attacks on VMs.

Just like physical network adapters, virtual machine network adapters can impersonate another VM. Impersonation is a security risk.

- A VM can send frames that appear to be from a different machine so that it can receive network frames that are intended for that machine.
- A virtual machine network adapter can be configured so that it receives frames targeted for other machines

When you add a VMkernel port group or virtual machine port group to a standard switch, ESXi configures a security policy for the ports in the group. You can use this security policy to ensure that the host prevents the guest operating systems of its VMs from impersonating other machines on the network. The guest operating system that might attempt impersonation does not detect that the impersonation was prevented.

The security policy determines how strongly you enforce protection against impersonation and interception attacks on VMs. To correctly use the settings in the security profile, see the Security Policy section in the *vSphere Networking* publication. This section explains:

- How VM network adapters control transmissions.
- How attacks are staged at this level

Securing vSphere Standard Switches

You can secure standard switch traffic against Layer 2 attacks by restricting some of the MAC address modes of the VM network adapters.

Each VM network adapter has an initial MAC address and an effective MAC address.

Initial MAC address	The initial MAC address is assigned when the adapter is created. Although the initial MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system.
Effective MAC address	Each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address that is different from the effective MAC address. The guest operating system is responsible for setting the effective MAC address and typically matches the effective MAC address to the initial MAC address.

Upon creating a VM network adapter, the effective MAC address and initial MAC address are the same. The guest operating system can alter the effective MAC address to another value at any time. If an operating system changes the effective MAC address, its network adapter receives network traffic that is destined for the new MAC address.

When sending packets through a network adapter, the guest operating system typically places its own adapter effective MAC address in the source MAC address field of the Ethernet frames. It places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only if the destination MAC address in the packet matches its own effective MAC address.

An operating system can send frames with an impersonated source MAC address. An operating system can therefore impersonate a network adapter that the receiving network authorizes, and stage malicious attacks on the devices in a network.

Protect virtual traffic against impersonation and interception Layer 2 attacks by configuring a security policy on port groups or ports.

The security policy on distributed port groups and ports includes the following options:

- MAC address changes (see MAC Address Changes)
- Promiscuous mode (see Promiscuous Mode Operation)
- Forged transmits (see Forged Transmits)

You can view and change the default settings by selecting the virtual switch associated with the host from the vSphere Client. See *vSphere Networking* documentation.

MAC Address Changes

The security policy of a virtual switch includes a **MAC address changes** option. This option allows virtual machines to receive frames with a Mac Address that is different from the one configured in the VMX.

When the **Mac address changes** option is set to **Accept**, ESXi accepts requests to change the effective MAC address of a virtual machine to a different address than the initial MAC address.

When the **Mac address changes** option is set to **Reject**, ESXi does not honor requests to change the effective MAC address of a virtual machine to a different address than the initial MAC address. This setting protects the host against MAC impersonation. The port that the virtual machine adapter used to send the request is disabled and the virtual machine adapter does not receive any more frames until the effective MAC address matches the initial MAC address. The guest operating system does not detect that the MAC address change request was not honored.

Note: The iSCSI initiator relies on being able to get MAC address changes from certain types of storage. If you are using ESXi iSCSI with iSCSI storage, set the **MAC address changes** option to **Accept**.

In some situations, you can have a legitimate need for more than one adapter to have the same MAC address on a network, for example, if you are using Microsoft Network Load Balancing in unicast mode. When Microsoft Network Load Balancing is used in the standard multicast mode, adapters do not share MAC addresses.

Note: Starting in vSphere 7.0, the defaults for **Forged transmits** and **MAC address changes** have been changed to Reject instead of Accept. Contact your storage vendor to validate.

Forged Transmits

The **Forged transmits** option affects traffic that is transmitted from a virtual machine.

When the **Forged transmits** option is set to **Accept**, ESXi does not compare source and effective MAC addresses.

To protect against MAC impersonation, you can set the **Forged transmits** option to **Reject**. If you do, the host compares the source MAC address being transmitted by the guest operating system with the effective MAC address for its virtual machine adapter to see if they match. If the addresses do not match, the ESXi host drops the packet.

The guest operating system does not detect that its virtual machine adapter cannot send packets by using the impersonated MAC address. The ESXi host intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets are dropped.

Note: Starting in vSphere 7.0, the defaults for **Forged transmits** and **MAC address changes** have been changed to Reject instead of Accept.

Promiscuous Mode Operation

Promiscuous mode eliminates any reception filtering that the virtual machine adapter performs so that the guest operating system receives all traffic observed on the wire. By default, the virtual machine adapter cannot operate in promiscuous mode.

Although promiscuous mode can be useful for tracking network activity, it is an insecure mode of operation, because any adapter in promiscuous mode has access to the packets even if some of the packets are received only by a particular network adapter. This means that an administrator or root user within a virtual machine can potentially view traffic destined for other guest or host operating systems.

See the topic on configuring the security policy for a vSphere Standard Switch or Standard Port Group in the *vSphere Networking* documentation for information about configuring the virtual machine adapter for promiscuous mode.

Note: In some situations, you might have a legitimate reason to configure a standard or a distributed virtual switch to operate in promiscuous mode, for example, if you are running network intrusion detection software or a packet sniffer.

Standard Switch Protection and VLANs

VMware standard switches provide safeguards against certain threats to VLAN security. Because of the way that standard switches are designed, they protect VLANs against a variety of attacks, many of which involve VLAN hopping.

Having this protection does not guarantee that your virtual machine configuration is invulnerable to other types of attacks. For example, standard switches do not protect the physical network against these attacks; they protect only the virtual network.

Standard switches and VLANs can protect against the following types of attacks.

MAC flooding	Floods a switch with packets that contain MAC addresses tagged as having come from different sources. Many switches use a content-addressable memory table to learn and store the source address for each packet. When the table is full, the switch can enter a fully open state in which every incoming packet is broadcast on all ports, letting the attacker see all of the switch's traffic. This state might result in packet leakage across VLANs. Although VMware standard switches store a MAC address table, they do not get the MAC addresses from observable traffic and are not vulnerable to this type of attack.
802.1q and ISL tagging attacks	Force a switch to redirect frames from one VLAN to another by tricking the switch into acting as a trunk and broadcasting the traffic to other VLANs.

	VMware standard switches do not perform the dynamic trunking required for this type of attack and, therefore, are not vulnerable.
Double-encapsulation attacks	Occur when an attacker creates a double-encapsulated packet in which the VLAN identifier in the inner tag is different from the VLAN identifier in the outer tag. For backward compatibility, native VLANs strip the outer tag from transmitted packets unless configured to do otherwise. When a native VLAN switch strips the outer tag, only the inner tag is left, and that inner tag routes the packet to a different VLAN than the one identified in the now-missing outer tag. VMware standard switches drop any double-encapsulated frames that a virtual machine attempts to send on a port configured for a specific VLAN. Therefore, they are not vulnerable to this type of attack.
Multicast brute-force attacks	Involve sending large numbers of multicast frames to a known VLAN almost simultaneously to overload the switch so that it mistakenly allows some of the frames to broadcast to other VLANs. VMware standard switches do not allow frames to leave their correct broadcast domain (VLAN) and are not vulnerable to this type of attack.
Spanning-tree attacks	Target Spanning-Tree Protocol (STP), which is used to control bridging between parts of the LAN. The attacker sends Bridge Protocol Data Unit (BPDU) packets that attempt to change the network topology, establishing themselves as the root bridge. As the root bridge, the attacker can sniff the contents of transmitted frames. VMware standard switches do not support STP and are not vulnerable to this type of attack.
Random frame attacks	Involve sending large numbers of packets in which the source and destination addresses stay the same, but in which fields are randomly changed in length, type, or content. The goal of this attack is to force packets to be mistakenly rerouted to a different VLAN. VMware standard switches are not vulnerable to this type of attack.

Because new security threats develop over time, do not consider this an exhaustive list of attacks. Regularly check VMware security resources on the Web to learn about security, recent security alerts, and VMware security tactics.

Secure vSphere Distributed Switches and Distributed Port Groups

Administrators have several options for securing vSphere Distributed Switches in their vSphere environment.

The same rules apply for VLANs in a vSphere Distributed Switch as they do in a standard switch. For more information, see Standard Switch Protection and VLANs.

1. For distributed port groups with static binding, disable the Auto Expand feature.

   Auto Expand is enabled by default in vSphere 5.1 and later.

   To disable Auto Expand, configure the `autoExpand` property under the distributed port group with the vSphere Web Services SDK or with a command-line interface. See the *vSphere Web Services SDK* documentation.

2. Ensure that all private VLAN IDs of any vSphere Distributed Switch are fully documented.
3. If you are using VLAN tagging on a dvPortgroup, VLAN IDs must correspond to the IDs on external VLAN-aware upstream switches. If VLAN IDs are not tracked correctly, mistaken reuse of IDs might allow unintended traffic. Similarly, wrong or missing VLAN IDs might lead to traffic not passing between physical and virtual machines.
4. Ensure that no unused ports exist on a virtual port group associated with a vSphere Distributed Switch.
5. Label all vSphere Distributed Switches.

   vSphere Distributed Switches associated with an ESXi host require a text box for the name of the switch. This label serves as a functional descriptor for the switch, just like the host name associated with a physical switch. The label on the vSphere Distributed Switch indicates the function or the IP subnet of the switch. For example, you can label the switch as internal to indicate that it is only for internal networking on a virtual machine's private virtual switch. No traffic goes over physical network adapters.
6. Disable network health check for your vSphere Distributed Switches if you are not actively using it.

   Network health check is disabled by default. Once enabled, the health check packets contain information about the host, switch, and port that an attacker can potentially use. Use network health check only for troubleshooting, and turn it off when troubleshooting is finished.
7. Protect virtual traffic against impersonation and interception Layer 2 attacks by configuring a security policy on port groups or ports.

   The security policy on distributed port groups and ports includes the following options:

   - MAC address changes (see MAC Address Changes)
   - Promiscuous mode (see Promiscuous Mode Operation)
   - Forged transmits (see Forged Transmits)

   You can view and change the current settings by selecting **Manage Distributed Port Groups** from the right-button menu of the distributed switch and selecting **Security** in the wizard. See the *vSphere Networking* documentation.

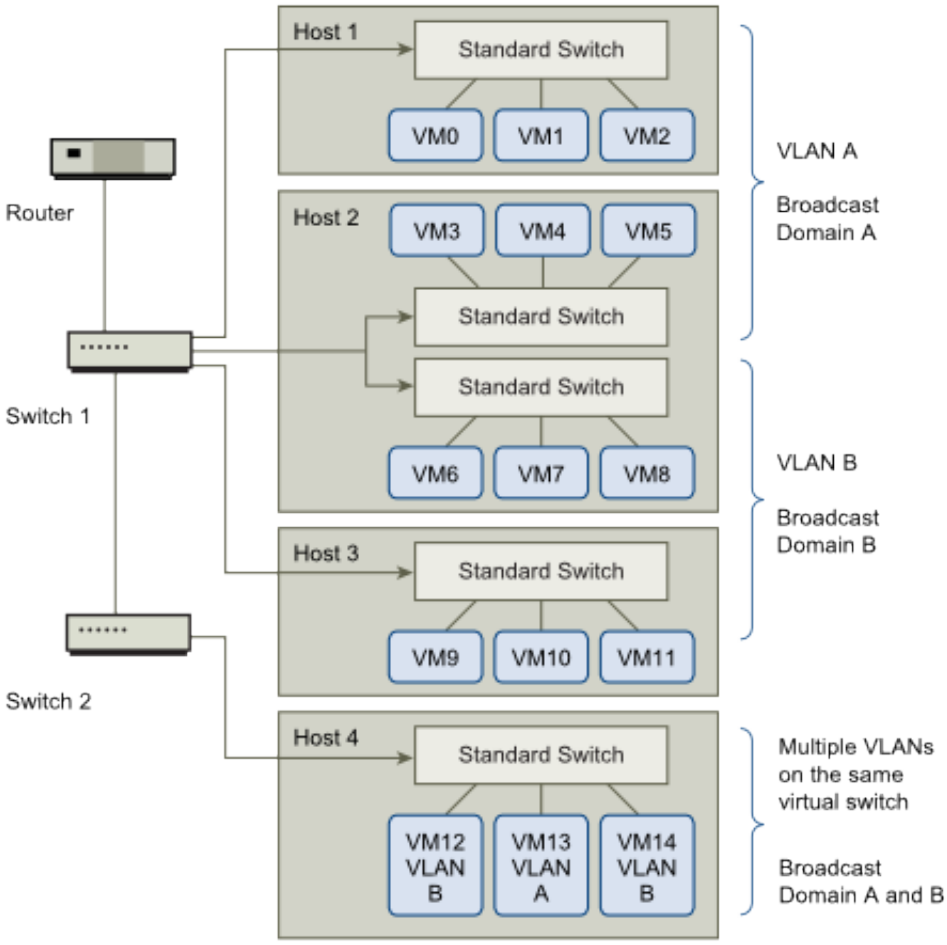
Securing Virtual Machines with VLANs

The network can be one of the most vulnerable parts of any system. Your virtual machine network requires as much protection as your physical network. Using VLANs can improve networking security in your environment.

VLANs are an IEEE standard networking scheme with specific tagging methods that allow routing of packets to only those ports that are part of the VLAN. When properly configured, VLANs provide a dependable means for you to protect a set of virtual machines from accidental or malicious intrusions.

VLANs let you segment a physical network so that two machines in the network are unable to transmit packets back and forth unless they are part of the same VLAN. For example, accounting records and transactions are among a company's most sensitive internal information. In a company whose sales, shipping, and accounting employees all use virtual machines in the same physical network, you might protect the virtual machines for the accounting department by setting up VLANs.

Figure 94: Sample VLAN Layout



In this configuration, all employees in the accounting department use virtual machines in VLAN A and the employees in sales use virtual machines in VLAN B.

The router forwards packets containing accounting data to the switches. These packets are tagged for distribution to VLAN A only. Therefore, the data is confined to Broadcast Domain A and cannot be routed to Broadcast Domain B unless the router is configured to do so.

This VLAN configuration prevents the sales force from intercepting packets destined for the accounting department. It also prevents the accounting department from receiving packets intended for the sales group. The virtual machines serviced by a single virtual switch can be in different VLANs.

Security Considerations for VLANs

The way you set up VLANs to secure parts of a network depends on factors such as the guest operating system and the way your network equipment is configured.

ESXi features a complete IEEE 802.1q-compliant VLAN implementation. VMware cannot make specific recommendations on how to set up VLANs, but there are factors to consider when using a VLAN deployment as part of your security enforcement policy.

Secure VLANs

Administrators have several options for securing the VLANs in their vSphere environment.

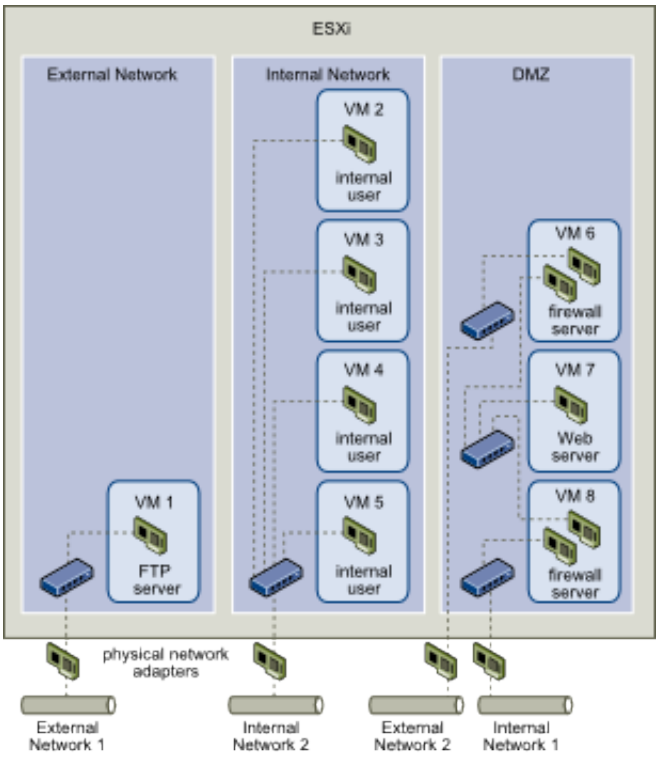
1. Ensure that port groups are not configured to VLAN values that are reserved by upstream physical switches
   Do not set VLAN IDs to values reserved for the physical switch.
2. Ensure that port groups are not configured to VLAN 4095 unless you are using for Virtual Guest Tagging (VGT).
   Three types of VLAN tagging exist in vSphere:
   - External Switch Tagging (EST)
   - Virtual Switch Tagging (VST) - The virtual switch tags with the configured VLAN ID the traffic that is incoming to the attached virtual machines and removes the VLAN tag from the traffic that is leaving them. To set up VST mode, assign a VLAN ID between 1 and 4094.
   - Virtual Guest Tagging (VGT) - Virtual machines handle VLAN traffic. To activate VGT mode, set the VLAN ID to 4095. On a distributed switch, you can also allow virtual machine traffic based on its VLAN by using the **VLAN Trunking** option.

   On a standard switch you can configure VLAN networking mode at switch or port group level, and on a distributed switch at distributed port group or port level.
3. Ensure that all VLANs on each virtual switch are fully documented and that each virtual switch has all required VLANs and only required VLANs.

Creating Multiple Networks Within a Single ESXi Host

The ESXi system is designed so that you can connect some groups of virtual machines to the internal network, others to the external network, and still others to both—all on the same host. This capability is an outgrowth of basic virtual machine isolation coupled with a well-planned use of virtual networking features.

Figure 95: External Networks, Internal Networks, and a DMZ Configured on a Single ESXi Host



In the figure, the system administrator configured a host into three distinct virtual machine zones: FTP server, internal virtual machines, and DMZ. Each zone serves a unique function.

FTP server	Virtual Machine 1 is configured with FTP software and acts as a holding area for data sent to and from outside resources such as forms and collateral localized by a vendor. This virtual machine is associated with an external network only. It has its own virtual switch and physical network adapter that connect it to External Network 1. This network is dedicated to servers that the company uses to receive data from outside sources. For example, the company uses External Network 1 to receive FTP traffic from vendors and allow vendors access to data stored on externally available servers though FTP. In addition to servicing Virtual Machine 1, External Network 1 services FTP servers configured on different ESXi hosts throughout the site. Because Virtual Machine 1 does not share a virtual switch or physical network adapter with any virtual machines in the host, the other resident virtual machines cannot transmit packets to or receive packets from the Virtual Machine 1 network. This restriction prevents sniffing attacks, which require sending network traffic to the victim. More importantly, an attacker cannot use the natural vulnerability of FTP to access any of the host's other virtual machines.
Internal virtual machines	Virtual Machines 2 through 5 are reserved for internal use. These virtual machines process and store company-private data such as medical records, legal settlements, and fraud investigations. As a result, the system administrators must ensure the highest level of protection for these virtual machines. These virtual machines connect to Internal Network 2 through their own virtual switch and network adapter. Internal Network 2 is reserved for internal use by personnel such as claims processors, in-house lawyers, or adjustors. Virtual Machines 2 through 5 can communicate with one another through the virtual switch and with internal virtual machines elsewhere on Internal Network 2 through the physical network adapter. They cannot communicate with externally facing machines. As with the FTP server, these virtual machines cannot send packets to or receive packets from the other virtual machines' networks. Similarly, the host's other virtual machines cannot send packets to or receive packets from Virtual Machines 2 through 5.
DMZ	Virtual Machines 6 through 8 are configured as a DMZ that the marketing group uses to publish the company's external website. This group of virtual machines is associated with External Network 2 and Internal Network 1. The company uses External Network 2 to support the Web servers that use the marketing and financial department to host the corporate website and other Web facilities that it hosts to outside users. Internal Network 1 is the conduit that the marketing department uses to publish its content to the corporate Web site, post downloads, and maintain services like user forums. Because these networks are separate from External Network 1 and Internal Network 2, and the virtual machines have no shared points of contact (switches or adapters), there is no risk of attack to or from the FTP server or the internal virtual machine group.

By capitalizing on virtual machine isolation, correctly configuring virtual switches, and maintaining network separation, the system administrator can house all three virtual machine zones in the same ESXi host and be confident that there will be no data or resource breaches.

The company enforces isolation among the virtual machine groups by using multiple internal and external networks and making sure that the virtual switches and physical network adapters for each group are separate from those of other groups.

Because none of the virtual switches straddle virtual machine zones, the system administrator succeeds in eliminating the risk of packet leakage from one zone to another. A virtual switch, by design, cannot leak packets directly to another virtual switch. The only way for packets to travel from one virtual switch to another is under the following circumstances:

- The virtual switches are connected to the same physical LAN.
- The virtual switches connect to a common virtual machine, which might be used to transmit packets.

Neither of these conditions occur in the sample configuration. If system administrators want to verify that no common virtual switch paths exist, they can check for possible shared points of contact by reviewing the network switch layout in the vSphere Client.

To safeguard the virtual machines' resources, the system administrator lowers the risk of DoS and DDoS attacks by configuring a resource reservation and a limit for each virtual machine. The system administrator further protects the ESXi host and virtual machines by installing software firewalls at the front and back ends of the DMZ, ensuring that the host is behind a physical firewall, and configuring the networked storage resources so that each has its own virtual switch.

Internet Protocol Security

Internet Protocol Security (IPsec) secures IP communications coming from and arriving at a host. ESXi hosts support IPsec using IPv6.

When you set up IPsec on a host, you enable authentication and encryption of incoming and outgoing packets. When and how IP traffic is encrypted depends on how you set up the system's security associations and security policies.

A security association determines how the system encrypts traffic. When you create a security association, you specify the source and destination, encryption parameters, and a name for the security association.

A security policy determines when the system should encrypt traffic. The security policy includes source and destination information, the protocol and direction of traffic to be encrypted, the mode (transport or tunnel) and the security association to use.

List Available Security Associations

ESXi can provide a list of all security associations available for use by security policies. The list includes both user created security associations and any security associations the VMkernel installed using Internet Key Exchange.

You can get a list of available security associations using the `esxcli` command.

At the command prompt, enter the command `esxcli network ip ipsec sa list`.

ESXi displays a list of all available security associations.

Add an IPsec Security Association

Add a security association to specify encryption parameters for associated IP traffic.

You can add a security association using the `esxcli` command.

At the command prompt, enter the command `esxcli network ip ipsec sa add` with one or more of the following options.

Option	Description
--sa-source= ***source address***	Required. Specify the source address.
--sa-destination= ***destination address***	Required. Specify the destination address.
--sa-mode= ***mode***	Required. Specify the mode, either `transport` or `tunnel`.
--sa-spi= ***security parameter index***	Required. Specify the security parameter index. The security parameter index identifies the security association to the host. It must be a hexadecimal with a 0x prefix. Each security association you create must have a unique combination of protocol and security parameter index.
--encryption-algorithm= ***encryption algorithm***	Required. Specify the encryption algorithm using one of the following parameters. • `3des-cbc` • `aes128-cbc` • `null` (provides no encryption)
--encryption-key= ***encryption key***	Required when you specify an encryption algorithm. Specify the encryption key. You can enter keys as ASCII text or as a hexadecimal with a 0x prefix.
--integrity-algorithm= ***authentication algorithm***	Required. Specify the authentication algorithm, either `hmac-sha1` or `hmac-sha2-256`.
--integrity-key= ***authentication key***	Required. Specify the authentication key. You can enter keys as ASCII text or as a hexadecimal with a 0x prefix.
--sa-name=*name*	Required. Provide a name for the security association.

New Security Association Command

The following example contains extra line breaks for readability.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x697076367265616479 6c6f676f3364657363626f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

Remove an IPsec Security Association

You can remove a security association using the ESXCLI command.

Verify that the security association you want to use is not currently in use. If you try to remove a security association that is in use, the removal operation fails.

At the command prompt, enter the command `esxcli network ip ipsec sa remove --sa-name security_association_name`.

List Available IPsec Security Policies

You can list available security policies using the ESXCLI command.

At the command prompt, enter the command `esxcli network ip ipsec sp list`.

The host displays a list of all available security policies.

Create an IPSec Security Policy

Create a security policy to determine when to use the authentication and encryption parameters set in a security association. You can add a security policy using the ESXCLI command.

Before creating a security policy, add a security association with the appropriate authentication and encryption parameters as described in Add an IPsec Security Association.

At the command prompt, enter the command `esxcli network ip ipsec sp add` with one or more of the following options.

Option	Description
--sp-source= ***source address***	Required. Specify the source IP address and prefix length.
--sp-destination= ***destination address***	Required. Specify the destination address and prefix length.
--source-port= ***port***	Required. Specify the source port. The source port must be a number between 0 and 65535.
--destination-port= ***port***	Required. Specify the destination port. The source port must be a number between 0 and 65535.
--upper-layer-protocol= ***protocol***	Specify the upper layer protocol using one of the following parameters. • `tcp` • `udp` • `icmp6` • `any`
--flow-direction= ***direction***	Specify the direction in which you want to monitor traffic using either `in` or `out`.
--action= ***action***	Specify the action to take when traffic with the specified parameters is encountered using one of the following parameters. • `none`: Take no action. • `discard`: Do not allow data in or out. • `ipsec`: Use the authentication and encryption information supplied in the security association to determine whether the data comes from a trusted source.
--sp-mode= ***mode***	Specify the mode, either `tunnel` or `transport`.
--sa-name=*security association name*	Required. Provide the name of the security association for the security policy to use.
--sp-name=*name*	Required. Provide a name for the security policy.

New Security Policy Command

The following example includes extra line breaks for readability.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Remove an IPsec Security Policy

You can remove a security policy from the ESXi host using the ESXCLI command.

Verify that the security policy you want to use is not currently in use. If you try to remove a security policy that is in use, the removal operation fails.

At the command prompt, enter the command `esxcli network ip ipsec sp remove --sa-name` *`security policy name`*.

To remove all security policies, enter the command `esxcli network ip ipsec sp remove --remove-all`.

Ensure Proper SNMP Configuration

If SNMP is not properly configured, monitoring information can be sent to a malicious host. The malicious host can then use this information to plan an attack.

ESXi includes an SNMP agent that can send notifications (traps and informs) and receive `GET` , `GETBULK` , and `GETNEXT` requests. SNMP is not enabled by default. SNMP must be configured on each ESXi host. You can use ESXCLI, PowerCLI, or the vSphere Web Services SDK for configuration.

See the *vSphere Monitoring and Performance* documentation for detailed information about configuring SNMP, including SNMP v3. SNMP v3 provides stronger security than SNMP v1 or SNMP v2c, including key authentication and encryption. See *ESXCLI Reference* for more information about the `esxcli system snmp` command options.

1. To determine whether SNMP is used, run the following command.

   ```
   esxcli system snmp get
   ```

2. To enable SNMP, run the following command.

   ```
   esxcli system snmp set --enable true
   ```

3. To disable SNMP, run the following command.

   ```
   esxcli system snmp set --enable false
   ```

vSphere Networking Security Best Practices

Following networking security best practices helps ensure the integrity of your vSphere deployment.

General Networking Security Recommendations

Following general network security recommendations is the first step in securing your networking environment. You can then move on to special areas, such as securing the network with firewalls or using IPsec.

- Spanning Tree Protocol (STP) detects and prevents loops from forming in the network topology. VMware virtual switches prevent loops in other ways, but do not support STP directly. When network topology changes occur, some time is required (30–50 seconds) while the network relearns the topology. During that time, no traffic is allowed to pass.

To avoid these problems, network vendors have created features to enable switch ports to continue forwarding traffic. For more information, see the VMware knowledge base article at https://kb.vmware.com/kb/1003804. Consult your network vendor documentation for the proper network and networking hardware configurations.

- Ensure that Netflow traffic for a Distributed Virtual Switch is only sent to authorized collector IP addresses. Netflow exports are not encrypted and can contain information about the virtual network. This information increases the potential for sensitive information to be viewed and captured in transit by attackers. If Netflow export is required, verify that all Netflow target IP addresses are correct.
- Ensure that only authorized administrators have access to virtual networking components by using the role-based access controls. For example, give virtual machine administrators only access to port groups in which their virtual machines reside. Give network administrators access to all virtual networking components but no access to virtual machines. Limiting access reduces the risk of misconfiguration, whether accidental or malicious, and enforces key security concepts of separation of duties and least privilege.
- Ensure that port groups are not configured to the value of the native VLAN. Physical switches are often configured with a native VLAN, and that native VLAN is often VLAN 1 by default. ESXi does not have a native VLAN. Frames with VLAN specified in the port group have a tag, but frames with VLAN not specified in the port group are not tagged. This can cause a problem because virtual machines that are tagged with a 1 end up belonging to native VLAN of the physical switch.

  For example, frames on VLAN 1 from a Cisco physical switch are untagged because VLAN 1 is the native VLAN on that physical switch. However, frames from the ESXi host that are specified as VLAN 1 are tagged with a 1. As a result, traffic from the ESXi host that is destined for the native VLAN is not routed correctly because it is tagged with a 1 instead of being untagged. Traffic from the physical switch that is coming from the native VLAN is not visible because it is not tagged. If the ESXi virtual switch port group uses the native VLAN ID, traffic from virtual machines on that port is not visible to the native VLAN on the switch because the switch is expecting untagged traffic.
- Ensure that port groups are not configured to VLAN values reserved by upstream physical switches. Physical switches reserve certain VLAN IDs for internal purposes and often disallow traffic configured to these values. For example, Cisco Catalyst switches typically reserve VLANs 1001–1024 and 4094. Using a reserved VLAN might result in a denial of service on the network.
- Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT). Setting a port group to VLAN 4095 activates VGT mode. In this mode, the virtual switch passes all network frames to the virtual machine without modifying the VLAN tags, leaving it to the virtual machine to deal with them.
- Restrict port-level configuration overrides on a distributed virtual switch. Port-level configuration overrides are disabled by default. When overrides are enabled, you can use different security settings for a virtual machine than the port-group level settings. Certain virtual machines require unique configurations, but monitoring is essential. If overrides are not monitored, anyone who gains access to a virtual machine with a less secure distributed virtual switch configuration might attempt to exploit that access.
- Ensure that distributed virtual switch port mirror traffic is sent only to authorized collector ports or VLANs. A vSphere Distributed Switch can mirror traffic from one port to another to allow packet capture devices to collect specific traffic flows. Port mirroring sends a copy of all specified traffic in unencrypted format. This mirrored traffic contains the full data in the packets captured and can result in total compromise of that data if misdirected. If port mirroring is required, verify that all port mirror destination VLAN, port, and uplink IDs are correct.

Labeling Networking Components

Identifying the different components of your networking architecture is critical and helps ensure that no errors are introduced as your network grows.

Follow these best practices:

- Ensure that port groups are configured with a clear network label. These labels serve as a functional descriptor for the port group and help you identify each port group's function as the network becomes more complex.
- Ensure that each vSphere Distributed Switch has a clear network label that indicates the function or IP subnet of the switch. This label serves as a functional descriptor for the switch, just as physical switches require a host name. For

example, you can label the switch as internal to show that it is for internal networking. You cannot change the label for a standard virtual switch.

Document and Check the vSphere VLAN Environment

Check your VLAN environment regularly to avoid addressing problems. Fully document the VLAN environment and ensure that VLAN IDs are used only once. Your documentation can help with troubleshooting and is essential when you want to expand the environment.

1. Ensure that all vSwitch and VLANS IDs are fully documented

   If you are using VLAN tagging on a virtual switch, the IDs must correspond to the IDs on external VLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs might allow for traffic between the wrong physical and virtual machines. Similarly, if VLAN IDs are wrong or missing, traffic between physical and virtual machines might be blocked where you want traffic to pass.

2. Ensure that VLAN IDs for all distributed virtual port groups (dvPortgroup instances) are fully documented.

   If you are using VLAN tagging on a dvPortgroup the IDs must correspond to the IDs on external VLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs might allow for traffic between the wrong physical and virtual machines. Similarly, if VLAN IDs are wrong or missing, traffic between physical and virtual machines might be blocked where you want traffic to pass.

3. Ensure that private VLAN IDs for all distributed virtual switches are fully documented.

   Private VLANs (PVLANs) for distributed virtual switches require primary and secondary VLAN IDs. These IDs must correspond to the IDs on external PVLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs might allow for traffic between the wrong physical and virtual machines. Similarly, if PVLAN IDs are wrong or missing, traffic between physical and virtual machines might be blocked where you want traffic to pass.

4. Verify that VLAN trunk links are connected only to physical switch ports that function as trunk links.

   When connecting a virtual switch to a VLAN trunk port, you must properly configure both the virtual switch and the physical switch at the uplink port. If the physical switch is not properly configured, frames with the VLAN 802.1q header are forwarded to a switch that not expecting their arrival.

Adopting Network Isolation Practices

Network isolation practices bolster network security in your vSphere environment.

Isolate the Management Network

The vSphere management network provides access to the vSphere management interface on each component. Services running on the management interface provide an opportunity for an attacker to gain privileged access to the systems. Remote attacks are likely to begin with gaining access to this network. If an attacker gains access to the management network, it provides the staging ground for further intrusion.

Strictly control access to management network by protecting it at the security level of the most secure VM running on an ESXi host or cluster. No matter how the management network is restricted, administrators must have access to this network to configure the ESXi hosts and vCenter Server system.

Place the vSphere management port group in a dedicated VLAN on a common standard switch. Production (VM) traffic can share the standard switch if the vSphere management port group's VLAN is not used by production VMs.

Check that the network segment is not routed, except to networks where other management-related entities are found. Routing a network segment might make sense for vSphere Replication. In particular, make sure that production VM traffic cannot be routed to this network.

Strictly control access to management functionality by using one of the following approaches.

- To access the management network in especially sensitive environments, configure a controlled gateway or other controlled method. For example, require that administrators connect to the management network through a VPN. Allow access to the management network only to trusted administrators.
- Configure bastion hosts that run management clients.

Isolate Storage Traffic

Ensure that IP-based storage traffic is isolated. IP-based storage includes iSCSI and NFS. VMs might share virtual switches and VLANs with the IP-based storage configurations. This type of configuration might expose IP-based storage traffic to unauthorized VM users.

IP-based storage frequently is not encrypted. Anyone with access to this network can view IP-based storage traffic. To restrict unauthorized users from viewing IP-based storage traffic, logically separate the IP-based storage network traffic from the production traffic. Configure the IP-based storage adapters on separate VLANs or network segments from the VMkernel management network to limit unauthorized users from viewing the traffic.

Isolate vMotion Traffic

vMotion migration information is transmitted in plain text. Anyone with access to the network over which this information flows can view it. Potential attackers can intercept vMotion traffic to obtain the memory contents of a VM. They might also stage a MiTM attack in which the contents are modified during migration.

Separate vMotion traffic from production traffic on an isolated network. Set up the network to be nonroutable, that is, make sure that no layer-3 router is spanning this and other networks, to prevent outside access to the network.

Use a dedicated VLAN on a common standard switch for the vMotion port group. Production (VM) traffic can use the same standard switch if the vMotion port group's VLAN is not used by production VMs.

Isolate vSAN Traffic

When configuring your vSAN network, isolate vSAN traffic on its own Layer 2 network segment. You can perform this isolation by using dedicated switches or ports, or by using a VLAN.

Use Virtual Switches with the vSphere Network Appliance API Only If Required

Do not configure your host to send network information to a virtual machine unless you are using products that use the vSphere Network Appliance API (DvFilter). If the vSphere Network Appliance API is enabled, an attacker might attempt to connect a virtual machine to the filter. This connection might provide access to the network of other virtual machines on the host.

If you are using a product that uses this API, verify that the host is configured correctly. See the sections on DvFilter in *Developing and Deploying vSphere Solutions, vServices, and ESX Agents*. If your host is set up to use the API, make sure that the value of the `Net.DVFilterBindIpAddress` parameter matches the product that uses the API.

1. Browse to the host in the vSphere Client inventory.
2. Click **Configure**.
3. Under System, click **Advanced System Settings**.
4. Scroll down to `Net.DVFilterBindIpAddress` and verify that the parameter has an empty value.

   The order of parameters is not strictly alphabetical. Type `DVFilter` in the Filter text box to display all related parameters.

5. Verify the setting.
   - If you are not using DvFilter settings, make sure that the value is blank.
   - If you are using DvFilter settings, make sure that the value of the parameter is correct. The value must match the value that the product that uses the DvFilter is using.

Best Practices Involving Multiple vSphere Components

Some security best practices, such as setting up PTP or NTP in your environment, affect more than one vSphere component. Consider these recommendations when configuring your environment.

See Securing ESXi Hosts and Securing Virtual Machines for related information.

Synchronizing Clocks on the vSphere Network

Verify that all components on the vSphere network have their clocks synchronized. If the clocks on the physical machines in your vSphere network are not synchronized, SSL certificates and SAML tokens, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server`vmware-vpxd` service from starting.

Time inconsistencies in vSphere can cause the first boot of a component in your environment to fail at different services depending on where in the environment time is not accurate and when the time is synchronized. Problems most commonly occur when the target ESXi host for the destination vCenter Server is not synchronized with NTP or PTP. Similarly, issues can arise if the destination vCenter Server migrates to an ESXi host set to a different time due to fully automated DRS.

To avoid time synchronization issues, ensure that the following is correct before installing, migrating, or upgrading a vCenter Server instance.

- The target ESXi host where the destination vCenter Server is to be deployed is synchronized to NTP or PTP.
- The ESXi host running the source vCenter Server is synchronized to NTP or PTP.
- When upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, if the vCenter Server appliance is connected to an external Platform Services Controller, ensure the ESXi host running the external Platform Services Controller is synchronized to NTP or PTP.
- If you are upgrading or migrating from vSphere 6.5 or 6.7 to vSphere 7.0, verify that the source vCenter Server or vCenter Server appliance and external Platform Services Controller have the correct time.

Verify that any Windows host machine on which vCenter Server runs is synchronized with the Network Time Server (NTP) server. See the VMware knowledge base article at https://kb.vmware.com/s/article/1318.

To synchronize ESXi clocks with an NTP or a PTP server, you can use the VMware Host Client. For information about editing the time configuration of an ESXi host, see topic *Edit the Time Configuration of an ESXi Host in the VMware Host Client* in the *vSphere Single Host Management - VMware Host Client* documentation.

To learn how to change time synchronization settings for vCenter Server, see topic *Configure the System Time Zone and Time Synchronization Settings* in the *vCenter Server Configuration* documentation.

To learn how to edit the time configuration for a host by using the vSphere Client, see topic *Editing the Time Configuration Settings of a Host* in the *vCenter Server and Host Management* documentation.

Synchronize ESXi Clocks with a Network Time Server

Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

This task explains how to set up NTP from the VMware Host Client. You can instead use the `vicfg-ntp` vCLI command. See the *vSphere Command-Line Interface Reference*.

1. Start the VMware Host Client, and connect to the ESXi host.
2. Click **Configure**.
3. Under **System**, click **Time Configuration**, and click **Edit**.
4. Select **Use Network Time Protocol (Enable NTP client)**.
5. In the Add NTP Server text box, enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.
6. Optional: Set the startup policy and service status.
7. Click **OK**.

   The host synchronizes with the NTP server.

Related Links

Configuring Time Synchronization Settings in vCenter Server on page 1722

You can change the time synchronization settings in vCenter Server after deployment.

Configuring Time Synchronization Settings in vCenter Server

You can change the time synchronization settings in vCenter Server after deployment.

When you deploy vCenter Server, you can choose the time synchronization method to be either by using an NTP server or by using VMware Tools. In case the time settings in your vSphere network change, you can edit the vCenter Server and configure the time synchronization settings by using the commands in the appliance shell.

When you enable periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host.

After time synchronization occurs, VMware Tools checks once every minute to determine whether the clocks on the guest operating system and the host still match. If not, the clock on the guest operating system is synchronized to match the clock on the host.

Native time synchronization software, such as Network Time Protocol (NTP), is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred. You can use only one form of periodic time synchronization in vCenter Server. If you decide to use native time synchronization software, vCenter Server VMware Tools periodic time synchronization is disabled, and the reverse.

Related Links

Synchronize ESXi Clocks with a Network Time Server on page 1373

Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

Use VMware Tools Time Synchronization

You can set up vCenter Server to use VMware Tools time synchronization.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.

   The default user with super administrator role is root.

2. Run the command to enable VMware Tools time synchronization.
   ```
   timesync.set --mode host
   ```
3. Optional: Run the command to verify that you successfully applied the VMware Tools time synchronization.
   ```
   timesync.get
   ```
   The command returns that the time synchronization is in host mode.

The time of the appliance is synchronized with the time of the ESXi host.

Add or Replace NTP Servers in the vCenter Server Configuration

To set up the vCenter Server to use NTP-based time synchronization, you must add the NTP servers to the vCenter Server configuration.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Add NTP servers to the vCenter Server configuration by running the following `ntp.set` command.
   ```
   ntp.set --servers IP-addresses-or-host-names
   ```
   In this command, *`IP-addresses-or-host-names`* is a comma-separated list of IP addresses or host names of the NTP servers.
   This command removes the current NTP servers (if any) and adds the new NTP servers to the configuration. If the time synchronization is based on an NTP server, then the NTP daemon is restarted to reload the new NTP servers. Otherwise, this command replaces the current NTP servers in the NTP configuration with the new NTP servers you specify.
3. Optional: To verify that you successfully applied the new NTP configuration settings, run the following command.
   ```
   ntp.get
   ```
   The command returns a space-separated list of the servers configured for NTP synchronization. If the NTP synchronization is enabled, the command returns that the NTP configuration is in Up status. If the NTP synchronization is disabled, the command returns that the NTP configuration is in Down status.
4. Optional: To verify if the NTP server is reachable, run the following command.
   ```
   ntp.test --servers IP-addresses-or-host-names
   ```
   The command returns the status of the NTP servers.

If the NTP synchronization is disabled, you can configure the time synchronization settings in the vCenter Server to be based on an NTP server. See Synchronize the Time in vCenter Server with an NTP Server.

Synchronize the Time in vCenter Server with an NTP Server

You can configure the time synchronization settings in the vCenter Server to be based on an NTP server.

Set up one or more Network Time Protocol (NTP) servers in the vCenter Server configuration. See Add or Replace NTP Servers in the vCenter Server Configuration.

1. Access the appliance shell and log in as a user who has the administrator or super administrator role.
   The default user with super administrator role is root.
2. Run the command to enable NTP-based time synchronization.
   ```
   timesync.set --mode NTP
   ```
3. Optional: Run the command to verify that you successfully applied the NTP synchronization.
   ```
   timesync.get
   ```
   The command returns that the time synchronization is in NTP mode.

Storage Security Best Practices

Follow best practices for storage security, as outlined by your storage security provider. You can also take advantage of CHAP and mutual CHAP to secure iSCSI storage, mask and zone SAN resources, and configure Kerberos credentials for NFS 4.1.

See also the *Administering VMware vSAN* documentation.

Securing iSCSI Storage

The storage you configure for a host might include one or more storage area networks (SANs) that use iSCSI. When you configure iSCSI on a host, you can take measures to minimize security risks.

iSCSI supports accessing SCSI devices and exchanging data by using TCP/IP over a network port rather than through a direct connection to a SCSI device. An iSCSI transaction encapsulates blocks of raw SCSI data in iSCSI records and transmits the data to the requesting device or user.

iSCSI SANs support efficient use of the existing Ethernet infrastructure to provide hosts access to storage resources that they can dynamically share. iSCSI SANs are an economical storage solution for environments that rely on a common storage pool to serve many users. As with any networked system, your iSCSI SANs can be subject to security breaches.

Note: The requirements and procedures for securing an iSCSI SAN are similar for hardware iSCSI adapters associated with hosts and for iSCSI configured directly through the host.

Securing iSCSI Devices

To secure iSCSI devices, require that the ESXi host, or initiator, can authenticate to the iSCSI device, or target, whenever the host attempts to access data on the target LUN.

Authentication ensures that the initiator has the right to access a target. You grant this right when you configure authentication on the iSCSI device.

ESXi does not support Secure Remote Protocol (SRP), or public-key authentication methods for iSCSI. You can use Kerberos only with NFS 4.1.

ESXi supports both CHAP and Mutual CHAP authentication. The *vSphere Storage* documentation explains how to select the best authentication method for your iSCSI device and how to set up CHAP.

Ensure uniqueness of CHAP secrets. Set up a different mutual authentication secret for each host. If possible, set up a different secret for each client that to the ESXi host. Unique secrets ensure that an attacker cannot create another arbitrary host and authenticate to the storage device even if one host is compromised. With a shared secret, compromise of one host might allow an attacker to authenticate to the storage device.

Protecting an iSCSI SAN

When you plan your iSCSI configuration, take measures to improve the overall security of the iSCSI SAN. Your iSCSI configuration is only as secure as your IP network, so by enforcing good security standards when you set up your network, you help safeguard your iSCSI storage.

The following are some specific suggestions for enforcing good security standards.

Protect Transmitted Data

A primary security risk in iSCSI SANs is that an attacker might sniff transmitted storage data.

Take additional measures to prevent attackers from easily seeing iSCSI data. Neither the hardware iSCSI adapter nor ESXi iSCSI initiator encrypts the data that they transmit to and from the targets, making the data more vulnerable to sniffing attacks.

Allowing your virtual machines to share standard switches and VLANs with your iSCSI configuration potentially exposes iSCSI traffic to misuse by a virtual machine attacker. To help ensure that intruders cannot listen to iSCSI transmissions, make sure that none of your virtual machines can see the iSCSI storage network.

If you use a hardware iSCSI adapter, you can accomplish this by making sure that the iSCSI adapter and ESXi physical network adapter are not inadvertently connected outside the host by virtue of sharing a switch or some other means. If you configure iSCSI directly through the ESXi host, you can accomplish this by configuring iSCSI storage through a different standard switch than the one used by your virtual machines.

In addition to protecting the iSCSI SAN by giving it a dedicated standard switch, you can configure your iSCSI SAN on its own VLAN to improve performance and security. Placing your iSCSI configuration on a separate VLAN ensures that no devices other than the iSCSI adapter have visibility into transmissions within the iSCSI SAN. Also, network congestion from other sources cannot interfere with iSCSI traffic.

Secure iSCSI Ports

When you run iSCSI devices, ESXi does not open any ports that listen for network connections. This measure reduces the chances that an intruder can break into ESXi through spare ports and gain control over the host. Therefore, running iSCSI does not present any additional security risks at the ESXi end of the connection.

Any iSCSI target device that you run must have one or more open TCP ports to listen for iSCSI connections. If any security vulnerabilities exist in the iSCSI device software, your data can be at risk through no fault of ESXi. To lower this risk, install all security patches that your storage equipment manufacturer provides and limit the devices connected to the iSCSI network.

Masking and Zoning SAN Resources

You can use zoning and LUN masking to separate SAN activity and restrict access to storage devices.

You can protect access to storage in your vSphere environment by using zoning and LUN masking with your SAN resources. For example, you might manage zones defined for testing independently within the SAN so they do not interfere with activity in the production zones. Similarly, you might set up different zones for different departments.

When you set up zones, take into account any host groups that are set up on the SAN device.

Zoning and masking capabilities for each SAN switch and disk array and the tools for managing LUN masking are vendor specific.

See your SAN vendor's documentation and the *vSphere Storage* documentation.

Using Kerberos for NFS 4.1

With NFS version 4.1, ESXi supports the Kerberos authentication mechanism.

The RPCSEC_GSS Kerberos mechanism is an authentication service. It allows an NFS 4.1 client installed on ESXi to prove its identity to an NFS server before mounting an NFS share. The Kerberos security uses cryptography to work across an insecure network connection.

The ESXi implementation of Kerberos for NFS 4.1 provides two security models, krb5 and krb5i, that offer different levels of security.

- Kerberos for authentication only (krb5) supports identity verification.
- Kerberos for authentication and data integrity (krb5i), in addition to identity verification, provides data integrity services. These services help to protect the NFS traffic from tampering by checking data packets for any potential modifications.

Kerberos supports cryptographic algorithms that prevent unauthorized users from gaining access to NFS traffic. The NFS 4.1 client on ESXi attempts to use either the AES256-CTS-HMAC-SHA1-96 or AES128-CTS-HMAC-SHA1-96 algorithm to access a share on the NAS server. Before using your NFS 4.1 datastores, make sure that AES256-CTS-HMAC-SHA1-96 or AES128-CTS-HMAC-SHA1-96 are enabled on the NAS server.

The following table compares Kerberos security levels that ESXi supports.

Table 267: Types of Kerberos Security

		ESXi 6.0	ESXi 6.5 and later
Kerberos for authentication only (krb5)	Integrity checksum for RPC header	Yes with DES	Yes with AES
	Integrity checksum for RPC data	No	No
Kerberos for authentication and data integrity (krb5i)	Integrity checksum for RPC header	No krb5i	Yes with AES
	Integrity checksum for RPC data		Yes with AES

When you use Kerberos authentication, the following considerations apply:

- ESXi uses Kerberos with the Active Directory domain.
- As a vSphere administrator, you specify Active Directory credentials to provide access to NFS 4.1 Kerberos datastores for an NFS user. A single set of credentials is used to access all Kerberos datastores mounted on that host.
- When multiple ESXi hosts share the NFS 4.1 datastore, you must use the same Active Directory credentials for all hosts that access the shared datastore. To automate the assignment process, set the user in host profiles and apply the profile to all ESXi hosts.
- You cannot use two security mechanisms, AUTH_SYS and Kerberos, for the same NFS 4.1 datastore shared by multiple hosts.

Verify That Sending Host Performance Data to Guests Is Disabled

vSphere includes virtual machine performance counters on Windows operating systems where VMware Tools is installed. Performance counters allow virtual machine owners to do accurate performance analysis within the guest operating system. By default, vSphere does not expose host information to the guest virtual machine.

By default, the capability to send host performance data to a virtual machine is disabled. This default setting prevents a virtual machine from obtaining detailed information about the physical host. If a security breach of the virtual machine occurs, the setting does not make host data available to the attacker.

Note: The following procedure illustrates the basic process. Consider using ESXCLI or VMware PowerCLI commands for performing this task on all hosts simultaneously.

1. On the ESXi system that hosts the virtual machine, browse to the VMX file.

   Virtual machine configuration files are located in the `/vmfs/volumes/`*`datastore`* directory, where *`datastore`* is the name of the storage device where the virtual machine files are stored.

2. In the VMX file, verify that the following parameter is set.

   ```
   tools.guestlib.enableHostInfo=FALSE
   ```

3. Save and close the file.

You cannot retrieve performance information about the host from inside the guest virtual machine.

Setting Timeouts for the ESXi Shell and vSphere Client

To prevent intruders from using an idle session, set timeouts for the ESXi Shell and vSphere Client.

ESXi Shell Timeout

For the ESXi Shell, you can set the following timeouts from the vSphere Client and from the Direct Console User Interface (DCUI).

Availability Timeout	The availability timeout setting is the amount of time that can elapse before you must log in after the is enabled. After the timeout period, the service is disabled and users are not allowed to log in.
Idle Timeout	The idle timeout is the amount of time that can elapse before the user is logged out of an idle interactive sessions. Changes to the idle timeout apply the next time a user logs in to the . Changes do not affect existing sessions.

vSphere Client Timeout

vSphere Client sessions end after 120 minutes by default. To change the default:

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab, and under **Settings**, select **General**.
3. Click **Edit**.
4. Select **Timeout settings**.
5. Enter your choices and click **Save**.

Managing TLS Protocol Configuration with the TLS Configurator Utility

vSphere enables only TLS by default. TLS 1.0 and TLS 1.1 are disabled by default. Whether you do a fresh install, upgrade, or migration, vSphere disables TLS 1.0 and TLS 1.1. You can use the TLS Configurator utility to enable older versions of the protocol temporarily on vSphere systems. You can then disable the older less secure versions after all connections use TLS 1.2.

Before you perform a reconfiguration, consider your environment. Depending on your environmental requirements and software versions, you might need to re-enable TLS 1.0 and TLS 1.1, in addition to TLS 1.2, to maintain interoperability. For VMware products, see the VMware Knowledge Base article at https://kb.vmware.com/s/article/2145796 for a list of VMware products that support TLS 1.2. For third-party integration, consult your vendor's documentation. The TLS Configurator utility works with vSphere 7.0 and prior releases, including 6.7, 6.5, and 6.0.

Ports That Support Disabling TLS Versions

When you run the TLS Configurator utility in the vSphere environment, you can disable TLS across ports that use TLS on vCenter Server and ESXi hosts. You can disable TLS 1.0 or both TLS 1.0 and TLS 1.1.

Starting in vSphere 7.0, vCenter Server runs two reverse proxy services:

- VMware reverse proxy service, `rhttpproxy`
- Envoy

Envoy is an open source edge and service proxy. Envoy owns port 443, and all incoming vCenter Server requests are routed through Envoy. In vSphere 7.0, `rhttpproxy` serves as a configuration management server for Envoy. As a result, the TLS configuration is applied to `rhttpproxy` , which in turn sends the configuration to Envoy.

vCenter Server and ESXi use ports that can be enabled or disabled for TLS protocols. The TLS Configuration utility `scan` option displays which versions of TLS are enabled for each service. See Scan vCenter Server for Enabled TLS Protocols.

For the list of all supported ports and protocols in VMware products, including vSphere and vSAN, see the VMware Ports and Protocols Tool™ at https://ports.vmware.com/. You can search ports by VMware product, create a customized list of ports, and print or save port lists.

Notes and Caveats

- The vSphere 6.7 release was the final release of vCenter Server for Windows. See the *vSphere Security* documentation for the 6.7 version of the product for information about reconfiguring TLS for Update Manager ports on vCenter Server for Windows.
- You can use TLS 1.2 to encrypt the connection between vCenter Server and an external Microsoft SQL Server. You cannot use a TLS 1.2 only connection to an external Oracle database. See the VMware Knowledge Base article at https://kb.vmware.com/kb/2149745.
- For vSphere 6.7 and earlier releases, do not disable TLS 1.0 on a vCenter Server or Platform Services Controller instance that is running on Windows Server 2008. Windows 2008 supports only TLS 1.0. See the Microsoft TechNet Article *TLS/SSL Settings* in the *Server Roles and Technologies Guide*.
- If you change the TLS protocols, you must restart the ESXi host to apply the changes. You must restart the host even if you apply the changes through the cluster configuration by using host profiles. You can choose to restart the host immediately, or postpone the restart to a more convenient time.

Enabling or Disabling TLS Versions in vSphere

Disabling TLS versions is a multi-phase process. Disabling TLS versions in the right order ensures that your environment stays up and running during the process.

You have two choices for using TLS in your environment.

- Disable TLS 1.0, and enable TLS 1.1 and TLS 1.2.
- Disable TLS 1.0 and TLS 1.1, and enable TLS 1.2.

vSphere Lifecycle Manager is always included with the vCenter Server system and the script updates the corresponding port.

1. Run the TLS Configurator utility on vCenter Server.
2. Run the TLS Configurator utility on each ESXi host that is managed by the vCenter Server. You can perform this task for each host or for all hosts in a cluster.

Perform an Optional Manual Backup

The TLS Configuration utility performs a backup each time the script modifies vCenter Server. If you need a backup to a specific directory, you can perform a manual backup.

Backup of the ESXi configuration is not supported.

For vCenter Server, the default directory is `/tmp/`*`yearmonthday`*`T`*`time`*.

1. Change directory to `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`.
2. To make a backup to a specific directory, run the following command.

```
directory_path/VcTlsReconfigurator> ./reconfigureVc backup -d backup_directory_path
```

3. Verify that the backup was successful.

   A successful backup looks similar to the following example. The order of services displayed might be different each time you run the `reconfigureVc backup` command, due to the way the command runs.

   ```
   vCenter Transport Layer Security reconfigurator, version=7.0.0, build=15518531
   For more information refer to the following article: https://kb.vmware.com/kb/2147469
   Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
   ================= Backing up vCenter Server TLS configuration ==================
   Using backup directory: /tmp/20200206T183550
   Backing up: vmware-rbd-watchdog
   Backing up: vmware-vpxd
   Backing up: vmcam
   Backing up: vmware-stsd
   Backing up: vmdird
   Backing up: vmware-sps
   Backing up: vmware-rhttpproxy
   Backing up: vami-lighttp
   Backing up: vmware-updatemgr
   Backing up: rsyslog
   ```

4. Optional: If you later have to perform a restore, you can run the following command.

   ```
   reconfigureVc restore -d optional_custom_backup_directory_path
   ```

Enable or Disable TLS Versions on vCenter Server Systems

You can use the TLS Configuration utility to enable or disable TLS versions on vCenter Server systems. As part of the process, you can disable TLS 1.0, and enable TLS 1.1 and TLS 1.2. Or, you can disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2.

Ensure that the hosts and services that the vCenter Server manages can communicate using a version of TLS that remains enabled. For products that communicate only using TLS 1.0, connectivity becomes unavailable.

1. Log in to the vCenter Server system with the user name and password for administrator@vsphere.local, or as another member of the vCenter Single Sign-On Administrators group who can run scripts.
2. Go to the directory where the script is located.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
   ```

3. Run the command, depending on which version of TLS you want to use.

   Note: The following commands restart the vCenter Server services.

   - To disable TLS 1.0 and enable both TLS 1.1 and TLS 1.2, run the following command.

     ```
     directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2
     ```

   - To disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2, run the following command.

     ```
     directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
     ```

4. If your environment includes other vCenter Server systems, repeat the process on each vCenter Server system.
5. Repeat the configuration on each ESXi host.

Enable or Disable TLS Versions on ESXi Hosts

You can use the TLS Configuration utility to enable or disable TLS versions on an ESXi host. As part of the process, you can disable TLS 1.0, and enable TLS 1.1 and TLS 1.2. Or, you can disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2.

Ensure that any products or services associated with the ESXi host can communicate using TLS 1.1 or TLS 1.2. For products that communicate only using TLS 1.0, connectivity is lost.

The Bash shell must be enabled on the vCenter Server Appliance.

For ESXi hosts, you use a different utility than for the other components of your vSphere environment. The utility is release-specific, and cannot be used on a previous release.

You can write a script to configure multiple hosts.

1. Using SSH, connect to the vCenter Server Appliance with the user name and password of the vCenter Single Sign-On user who can run scripts.
2. To enable the Bash shell, enter `shell` at the command line.
3. Go to the directory where the script is located.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator
   ```

4. For an ESXi host that is part of a cluster, run one of the following commands.
   - To disable TLS 1.0 and enable both TLS 1.1 and TLS 1.2 on all hosts in a cluster, run the following command.

     ```
     ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2
     ```

   - To disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2 on all hosts in a cluster, run the following command.

     ```
     ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2
     ```

5. For an individual host that is not part of a cluster, run one of the following commands.
   - To disable TLS 1.0 and enable both TLS 1.1 and TLS 1.2 for an individual host, run the following command.

     ```
     ./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.1 TLSv1.2
     ```

   - To disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2 for an individual host, run the following command.

     ```
     ./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.2
     ```

     Note: To reconfigure a standalone ESXi host, log into a vCenter Server system and run the `reconfigureEsx` command with the ESXiHost-h*HOST*-u*ESXi_USER* options. For the *HOST* option, you can specify the IP address or FQDN of a single ESXi host, or a list of host IP addresses or FQDNs. For example, logging in to a vCenter Server and running the following command enables both TLS 1.1 and TLS 1.2 on two ESXi hosts:

     ```
     ./reconfigureEsx ESXiHost -h 198.51.100.2 198.51.100.3 -u root -p TLSv1.1 TLSv1.2
     ```

     Alternatively, to reconfigure a standalone ESXi host, you can log into the host and modify the `UserVars.ESXiVPsDisabledProtocols` advanced setting. See the topic titled "Configure Advanced TLS/SSL Key Options" in the *vSphere Single Host Management - VMware Host Client* documentation for more information.

6. Reboot the ESXi host to complete the TLS protocol changes.

Scan vCenter Server for Enabled TLS Protocols

After you enable or disable TLS versions on vCenter Server, you can use the TLS Configuration utility to view your changes.

The TLS Configuration utility `scan` option displays which versions of TLS are enabled for each service.

1. Log in to the vCenter Server system.
   a) Connect to the appliance using SSH and log in as a user who has privileges to run scripts.
   b) If the bash shell is not currently enabled, run the following commands.

      ```
      shell.set --enabled true
      shell
      ```

2. Go to the `VcTlsReconfigurator` directory.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
   ```

3. To display which services have TLS enabled, and the ports used, run the following command.

   ```
   ./reconfigureVc scan
   ```

Revert TLS Configuration Changes

You can use the TLS Configuration utility to revert configuration changes. When you revert the changes, the system enables protocols that you disabled using TLS Configurator utility.

Before reverting changes, use the vCenter Server Management interface to perform a backup of the vCenter Server.

1. Connect to the vCenter Server where you want to revert changes as a user who has privileges to run scripts.
2. If the Bash shell is not currently enabled, run the following commands.

   ```
   shell.set --enabled true
   shell
   ```

3. Go to the `VcTlsReconfigurator` directory.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
   ```

4. Review the previous backup.

   ```
   grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log
   ```

   The output looks like the following example.

   ```
   2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
   2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
   ```

5. Run the following command to perform a restore.

   ```
   reconfigureVc restore -d Directory_path_from_previous_step
   ```

   The output looks like the following example.

   ```
   2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
   2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
   ```

6. Repeat the procedure on any other vCenter Server instances.

Defined Privileges

The following tables list the default privileges that, when selected for a role, can be paired with a user and assigned to an object.

vCenter Server allows fine-grained control over authorization with permissions and roles. When you assign a permission to an object in the vCenter Server object hierarchy, you specify which user or group has which privileges on that object. To specify the privileges, you use roles, which are sets of privileges. For more information, see:

- Managing Permissions for vCenter Components
- Using Roles to Assign Privileges

When setting permissions, verify all the object types are set with appropriate privileges for each particular action. Some operations require access permission at the root folder or parent folder in addition to access to the object being manipulated. Some operations require access or performance permission at a parent folder and a related object.

vCenter Server extensions might define additional privileges not listed here. Refer to the documentation for the extension for more information on those privileges.

Alarms Privileges

Alarms privileges control the ability to create, modify, and respond to alarms on inventory objects.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 268: Alarms Privileges

Privilege Name	Description	Required On
Alarms > **Acknowledge alarm**	Allows suppression of all alarm actions on all triggered alarms.	Object on which an alarm is defined
Alarms > **Create alarm**	Allows creation of a new alarm. When creating alarms with a custom action, privilege to perform the action is verified when the user creates the alarm.	Object on which an alarm is defined
Alarms > **Disable alarm action**	Allows stopping an alarm action from occurring after an alarm has been triggered. This does not disable the alarm.	Object on which an alarm is defined
	Allows enabling or disabling a particular alarm on a particular target type.	
Alarms > **Modify alarm**	Allows changing the properties of an alarm.	Object on which an alarm is defined
Alarms > **Remove alarm**	Allows deletion of an alarm.	Object on which an alarm is defined
Alarms > **Set alarm status**	Allows changing the status of the configured event alarm. The status can change to **Normal**, **Warning**, or **Alert**.	Object on which an alarm is defined

Auto Deploy and Image Profile Privileges

Auto Deploy privileges control who can perform different tasks on Auto Deploy rules, and who can associate a host. Auto Deploy privileges also allow you to control who can create or edit an image profile.

The table describes privileges that determine who can manage Auto Deploy rules and rule sets and who can create and edit image profiles. See *vCenter Server Installation and Setup*.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 269: Auto Deploy Privileges

Privilege Name	Description	Required On
Auto Deploy > **Host** > **AssociateMachine**	Allows users to associate a host with a machine.	
Auto Deploy > **Image Profile** > **Create**	Allows creation of image profiles.	
Auto Deploy > **Image Profile** > **Edit**	Allows editing of image profiles.	
Auto Deploy > **Rule** > **Create**	Allows creation of Auto Deploy rules.	
Auto Deploy > **Rule** > **Delete**	Allows deletion of Auto Deploy rules.	
Auto Deploy > **Rule** > **Edit**	Allows editing of Auto Deploy rules.	

Privilege Name	Description	Required On
Auto Deploy > **RuleSet** > **Activate**	Allows activation of Auto Deploy rule sets.	
Auto Deploy > **RuleSet** > **Edit**	Allows editing of Auto Deploy rule sets.	

Certificates Privileges

Certificates privileges control which users can manage certificates.

This privilege determines who can perform certificate management for hosts. See Required Privileges for Certificate Management Operations in the *vSphere Authentication* documentation for information on vCenter Server certificate management.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 270: Host Certificates Privileges

Privilege Name	Description	Required On
Certificates > **Manage Certificates**	Allows certificate management for hosts.	vCenter Server

Certificate Authority Privileges

Certificate authority privileges control aspects of VMware Certificate Authority (VMCA) certificates.

Table 271: Certificate Authority Privileges

Privilege Name	Description	Required On
Certificate Authority > **Create/Delete (Admins priv).**	Allows full administrative-level access for managing vCenter Server certificates.	vCenter Server
Certificate Authority > **Create/Delete (below Admins priv).**	Allows viewing the VMCA root certificate in the Certificate Management page in the vSphere Client.	vCenter Server

Certificate Management Privileges

Certificate management privileges control which users can manage vCenter Server certificates.

Table 272: Certificate Management Privileges

Privilege Name	Description	Required On
	Allows full administrative-level access to various internal APIs and functionality for vCenter Server certificate-related operations.	vCenter Server
	Allows reduced administrative access to various internal APIs and functionality. This privilege restricts certificate related operations so that the user cannot escalate non-administrator privileges. Allowed operations are: • Generating certificate signing requests	vCenter Server

Privilege Name	Description	Required On
	• Creating and retrieving Trusted Root chains • Deleting Trusted Root chains created by a user with the privilege • Retrieving Machine SSL certificates • Retrieving the signing certificate chains for validating tokens issued by vCenter Server	

Cns Privileges

Cloud Native Store (Cns) privileges control which users can access the Cloud Native Storage UI.

Table 273: Cns Privileges

Privilege Name	Description	Required On
Cns > **Searchable**	Allows storage administrator to view the Cloud Native Storage UI.	Root vCenter Server

Content Library Privileges

Content Libraries provide simple and effective management for virtual machine templates and vApps. Content library privileges control who can view or manage different aspects of content libraries.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Note: Inheritance of permissions for content libraries works in the context of a single instance. However, content libraries are not direct children of a system from an inventory perspective. The direct parent for content libraries is the global root. This means that if you set a permission at a level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and so on, but does not apply to the content libraries that you see and operate with in this instance. To assign a permission on a content library, an Administrator must grant the permission to the user as a global permission. Global permissions support assigning privileges across solutions from a global root object.

Table 274: Content Library Privileges

Privilege Name	Description	Required On
Content library > **Add library item**	Allows addition of items in a library.	Library
	Allows addition of root certificates to the Trusted Root Certificates Store.	
	Allows checking in of templates.	Library
	Allows checking out of templates.	Library
Content library > **Create a subscription for a published library**	Allows creation of a library subscription.	Library
Content library > **Create local library**	Allows creation of local libraries on the specified system.	
	Allows creation or deletion of the VMware Tanzu Harbor Registry service.	for creation. Registry for deletion.

Privilege Name	Description	Required On
Content library > **Create subscribed library**	Allows creation of subscribed libraries.	
	Allows creation, deletion, or purging of VMware Tanzu Harbor Registry projects.	Registry
Content library > **Delete library item**	Allows deletion of library items.	Library. Set this permission to propagate to all library items.
Content library > **Delete local library**	Allows deletion of a local library.	Library
	Allows deletion of root certificates from the Trusted Root Certificates Store.	
Content library > **Delete subscribed library**	Allows deletion of a subscribed library.	Library
Content library > **Delete subscription of a published library**	Allows deletion of a subscription to a library.	Library
Content library > **Download files**	Allows download of files from the content library.	Library
Content library > **Evict library item**	Allows eviction of items. The content of a subscribed library can be cached or not cached. If the content is cached, you can release a library item by evicting it if you have this privilege.	Library. Set this permission to propagate to all library items.
Content library > **Evict subscribed library**	Allows eviction of a subscribed library. The content of a subscribed library can be cached or not cached. If the content is cached, you can release a library by evicting it if you have this privilege.	Library
Content library > **Import Storage**	Allows a user to import a library item if the source file URL starts with `ds://` or `file://`. This privilege is disabled for content library administrator by default. Because an import from a storage URL implies import of content, enable this privilege only if necessary and if no security concern exists for the user who performs the import.	Library
	Allows management of VMware Tanzu Harbor Registry resources.	Compute cluster
Content library > **Probe subscription information**	This privilege allows solution users and APIs to probe a remote library's subscription info including URL, SSL certificate, and password. The resulting structure describes whether the subscription configuration is successful or whether there are problems such as SSL errors.	Library
Content library > **Publish a library item to its subscribers**	Allows publication of library items to subscribers.	Library. Set this permission to propagate to all library items.
Content library > **Publish a library to its subscribers**	Allows publication of libraries to subscribers.	Library
Content library > **Read storage**	Allows reading of content library storage.	Library
Content library > **Sync library item**	Allows synchronization of library items.	Library. Set this permission to propagate to all library items.
Content library > **Sync subscribed library**	Allows synchronization of subscribed libraries.	Library
Content library > **Type introspection**	Allows a solution user or API to introspect the type support plug-ins for the content library service.	Library

Privilege Name	Description	Required On
Content library > **Update configuration settings**	Allows you to update the configuration settings. No vSphere Client user interface elements are associated with this privilege.	Library
Content library > **Update files**	Allows you to upload content into the content library. Also allows you to remove files from a library item.	Library
Content library > **Update library**	Allows updates to the content library.	Library
Content library > **Update library item**	Allows updates to library items.	Library. Set this permission to propagate to all library items.
Content library > **Update local library**	Allows updates of local libraries.	Library
Content library > **Update subscribed library**	Allows you to update the properties of a subscribed library.	Library
Content library > **Update subscription of a published library**	Allows updates of subscription parameters. Users can update parameters such as the subscribed library's vCenter Server instance specification and placement of its virtual machine template items.	Library
Content library > **View configuration settings**	Allows you to view the configuration settings. No vSphere Client user interface elements are associated with this privilege.	Library

Cryptographic Operations Privileges

Cryptographic operations privileges control who can perform which type of cryptographic operation on which type of object.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 275: Cryptographic Operations Privileges

Privilege Name	Description	Required On
Cryptographic operations > **Direct Access**	Allows users access to encrypted resources. Users can export virtual machines, have NFC access to virtual machines, and open a console session to an encrypted virtual machine.	Virtual machine, host, or datastore
Cryptographic operations > **Add disk**	Allows users to add a disk to an encrypted virtual machine.	Virtual machine
Cryptographic operations > **Clone**	Allows users to clone an encrypted virtual machine.	Virtual machine
Cryptographic operations > **Decrypt**	Allows users to decrypt a virtual machine or disk.	Virtual machine
Cryptographic operations > **Encrypt**	Allows users to encrypt a virtual machine or a virtual machine disk.	Virtual machine
Cryptographic operations > **Encrypt new**	Allows users to encrypt a virtual machine during virtual machine creation or a disk during disk creation.	Virtual machine folder

Privilege Name	Description	Required On
Cryptographic operations > **Manage encryption policies**	Allows users to manage virtual machine storage policies with encryption IO filters. By default, virtual machines that use the Encryption storage policy do not use other storage policies.	vCenter Server root folder
Cryptographic operations > **Manage KMS**	Allows users to manage the Key Management Server for the vCenter Server system. Management tasks include adding and removing KMS instances, and establishing a trust relationship with the KMS.	vCenter Server system
Cryptographic operations > **Manage keys**	Allows users to perform key management operations. These operations are not supported from the vSphere Client but can be performed by using `crypto-util` or the API.	vCenter Server root folder
Cryptographic operations > **Migrate**	Allows users to migrate an encrypted virtual machine to a different ESXi host. Supports migration with or without vMotion and storage vMotion. Supports migration to a different vCenter Server instance.	Virtual machine
Cryptographic operations > **Recrypt**	Allows users to recrypt virtual machines or disks with a different key. This privilege is required for both deep and shallow recrypt operations.	Virtual machine
Cryptographic operations > **Register VM**	Allows users to register an encrypted virtual machine with an ESXi host.	Virtual machine folder
Cryptographic operations > **Register host**	Allows users to enable encryption on a host. You can enable encryption on a host explicitly, or the virtual machine creation process can enable it.	Host folder for standalone hosts, cluster for hosts in cluster
Cryptographic operations > **Read Key Servers Info**	Allows users to list vSphere Native Key Providers on the vCenter Server and on hosts. Also allows users to get vSphere Native Key Provider information.	vCenter Server or host

dvPort Group Privileges

Distributed virtual port group privileges control the ability to create, delete, and modify distributed virtual port groups.

The table describes the privileges required to create and configure distributed virtual port groups.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 276: Distributed Virtual Port Group Privileges

Privilege Name	Description	Required On
dvPort group > **Create**	Allows creation of a distributed virtual port group.	Virtual port groups
dvPort group > **Delete**	Allows deletion of distributed virtual port group. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Virtual port groups
dvPort group > **Modify**	Allows modification of a distributed virtual port group configuration.	Virtual port groups
dvPort group > **Policy operation**	Allows setting the policy of a distributed virtual port group.	Virtual port groups
dvPort group > **Scope operation**	Allows setting the scope of a distributed virtual port group.	Virtual port groups

Distributed Switch Privileges

Distributed Switch privileges control the ability to perform tasks related to the management of Distributed Switch instances.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 277: vSphere Distributed Switch Privileges

Privilege Name	Description	Required On
Distributed switch > **Create**	Allows creation of a distributed switch.	Data centers, Network folders
Distributed switch > **Delete**	Allows removal of a distributed switch. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Distributed switches
Distributed switch > **Host operation**	Allows changing the host members of a distributed switch.	Distributed switches
Distributed switch > **Modify**	Allows changing the configuration of a distributed switch.	Distributed switches
Distributed switch > **Move**	Allows moving a vSphere Distributed Switch to another folder.	Distributed switches
Distributed switch > **Network I/O control operation**	Allow changing the resource settings for a vSphere Distributed Switch.	Distributed switches
Distributed switch > **Policy operation**	Allows changing the policy of a vSphere Distributed Switch.	Distributed switches
Distributed switch > **Port configuration operation**	Allow changing the configuration of a port in a vSphere Distributed Switch.	Distributed switches
Distributed switch > **Port setting operation**	Allows changing the setting of a port in a vSphere Distributed Switch.	Distributed switches
Distributed switch > **VSPAN operation**	Allows changing the VSPAN configuration of a vSphere Distributed Switch.	Distributed switches

Datacenter Privileges

Datacenter privileges control the ability to create and edit data centers in the vSphere Client inventory.

All data center privileges are used in vCenter Server only. The **Create datacenter** privilege is defined on data center folders or the root object. All other data center privileges are pair with data centers, data center folders, or the root object.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 278: Datacenter Privileges

Privilege Name	Description	Required On
Datacenter > **Create datacenter**	Allows creation of new data center.	Data center folder or root object
Datacenter > **Move datacenter**	Allows moving a data center. Privilege must be present at both the source and destination.	Data center, source and destination
Datacenter > **Network protocol profile configuration**	Allows configuration of the network profile for a data center.	Data center
Datacenter > **Query IP pool allocation**	Allows configuration of a pool of IP addresses.	Data center
Datacenter > **Reconfigure datacenter**	Allows reconfiguration of a data center.	Data center
Datacenter > **Release IP allocation**	Allows releasing the assigned IP allocation for a data center.	Data center
Datacenter > **Remove datacenter**	Allows removal of a data center. To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	Data center plus parent object
Datacenter > **Rename datacenter**	Allows changing the name of a data center.	Data center

Datastore Privileges

Datastore privileges control the ability to browse, manage, and allocate space on datastores.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 279: Datastore Privileges

Privilege Name	Description	Required On
Datastore > **Allocate space**	Allows allocating space on a datastore for a virtual machine, snapshot, clone, or virtual disk.	Data stores
Datastore > **Browse datastore**	Allows browsing files on a datastore.	Data stores
Datastore > **Configure datastore**	Allows configuration of a datastore.	Data stores
Datastore > **Low level file operations**	Allows performing read, write, delete, and rename operations in the datastore browser.	Data stores
Datastore > **Move datastore**	Allows moving a datastore between folders. Privileges must be present at both the source and destination.	Datastore, source and destination
Datastore > **Remove datastore**	Allows removal of a datastore. This privilege is deprecated.	Data stores

Privilege Name	Description	Required On
	To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	
Datastore > **Remove file**	Allows deletion of files in the datastore. This privilege is deprecated. Assign the **Low level file operations** privilege.	Data stores
Datastore > **Rename datastore**	Allows renaming a datastore.	Data stores
Datastore > **Update virtual machine files**	Allows updating file paths to virtual machine files on a datastore after the datastore has been resignatured.	Data stores
Datastore > **Update virtual machine metadata**	Allows updating virtual machine metadata associated with a datastore.	Data stores

Datastore Cluster Privileges

Datastore cluster privileges control the configuration of datastore clusters for Storage DRS.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 280: Datastore Cluster Privileges

Privilege Name	Description	Required On
Datastore cluster > **Configure a datatstore cluster**	Allows creation of and configuration of settings for datastore clusters for Storage DRS.	Datastore clusters

ESX Agent Manager Privileges

ESX Agent Manager privileges control operations related to ESX Agent Manager and agent virtual machines. The ESX Agent Manager is a service that lets you install management virtual machines, which are tied to a host and not affected by VMware DRS or other services that migrate virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 281: ESX Agent Manager

Privilege Name	Description	Required On
ESX Agent Manager > **Config**	Allows deployment of an agent virtual machine on a host or cluster.	Virtual machines
ESX Agent Manager > **Modify**	Allows modifications to an agent virtual machine such as powering off or deleting the virtual machine.	Virtual machines
ESX Agent View > **View**	Allows viewing of an agent virtual machine.	Virtual machines

Extension Privileges

Extension privileges control the ability to install and manage extensions.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 282: Extension Privileges

Privilege Name	Description	Required On
Extension > **Register extension**	Allows registration of an extension (plug-in).	Root vCenter Server
Extension > **Unregister extension**	Allows unregistering an extension (plug-in).	Root vCenter Server
Extension > **Update extension**	Allows updates to an extension (plug-in).	Root vCenter Server

External Stats Provider Privileges

External stats provider privileges control the ability to notify vCenter Server of Proactive Distributed Resource Scheduler (DRS) statistics.

These privileges apply to an API that is VMware-internal only.

Folder Privileges

Folder privileges control the ability to create and manage folders.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 283: Folder Privileges

Privilege Name	Description	Required On
Folder > **Create folder**	Allows creation of a new folder.	Folders
Folder > **Delete folder**	Allows deletion of a folder. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Folders
Folder > **Move folder**	Allows moving a folder. Privilege must be present at both the source and destination.	Folders
Folder > **Rename folder**	Allows changing the name of a folder.	Folders

Global Privileges

Global privileges control global tasks related to tasks, scripts, and extensions.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 284: Global Privileges

Privilege Name	Description	Required On
Global > **Act as vCenter Server**	Allows preparation or initiation of a vMotion send operation or a vMotion receive operation.	Root vCenter Server
Global > **Cancel task**	Allows cancellation of a running or queued task.	Inventory object related to the task
Global > **Capacity planning**	Allows enabling the use of capacity planning for planning consolidation of physical machines to virtual machines.	Root vCenter Server
Global > **Diagnostics**	Allows retrieval of a list of diagnostic files, log header, binary files, or diagnostic bundle. To avoid potential security breaches, limit this privilege to the vCenter Server Administrator role.	Root vCenter Server
Global > **Disable methods**	Allows servers for vCenter Server extensions to disable certain operations on objects managed by vCenter Server.	Root vCenter Server
Global > **Enable methods**	Allows servers for vCenter Server extensions to enable certain operations on objects managed byvCenter Server.	Root vCenter Server
Global > **Global tag**	Allows adding or removing global tags.	Root host or vCenter Server
Global > **Health**	Allows viewing the health of vCenter Server components.	Root vCenter Server
Global > **Licenses**	Allows viewing installed licenses and adding or removing licenses.	Root host or vCenter Server
Global > **Log event**	Allows logging a user-defined event against a particular managed entity.	Any object
Global > **Manage custom attributes**	Allows adding, removing, or renaming custom field definitions.	Root vCenter Server
Global > **Proxy**	Allows access to an internal interface for adding or removing endpoints to or from the proxy.	Root vCenter Server
Global > **Script action**	Allows scheduling a scripted action along with an alarm.	Any object
Global > **Service managers**	Allows use of the `resxtop` command in ESXCLI.	Root host or vCenter Server
Global > **Set custom attribute**	Allows viewing, creating, or removing custom attributes for a managed object.	Any object
Global > **Settings**	Allows reading and modifying runtime vCenter Server configuration settings.	Root vCenter Server
Global > **System tag**	Allows adding or removing system tags.	Root vCenter Server

Health Update Provider Privileges

Health update provider privileges control the ability for hardware vendors to notify vCenter Server of Proactive HA events.

These privileges apply to an API that is VMware-internal only.

Host CIM Privileges

Host CIM privileges control the use of CIM for host health monitoring.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 285: Host CIM Privileges

Privilege Name	Description	Required On
Host > **CIM** > **CIM Interaction**	Allow a client to obtain a ticket to use for CIM services.	Hosts

Host Configuration Privileges

Host configuration privileges control the ability to configure hosts.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 286: Host Configuration Privileges

Privilege Name	Description	Required On
Host > **Configuration** > **Advanced Settings**	Allows setting advanced host configuration options.	Hosts
Host > **Configuration** > **Authentication Store**	Allows configuring Active Directory authentication stores.	Hosts
Host > **Configuration** > **Change PciPassthru settings**	Allows changes to PciPassthru settings for a host.	Hosts
Host > **Configuration** > **Change SNMP settings**	Allows changes to SNMP settings for a host.	Hosts
Host > **Configuration** > **Change date and time settings**	Allows changes to date and time settings on the host.	Hosts
Host > **Configuration** > **Change settings**	Allows setting of lockdown mode on ESXi hosts.	Hosts
Host > **Configuration** > **Connection**	Allows changes to the connection status of a host (connected or disconnected).	Hosts
Host > **Configuration** > **Firmware**	Allows updates to the ESXi host's firmware.	Hosts
Host > **Configuration** > **Hyperthreading**	Allows enabling and disabling hyperthreading in a host CPU scheduler.	Hosts
Host > **Configuration** > **Image configuration**	Allows changes to the image associated with a host.	
Host > **Configuration** > **Maintenance**	Allows putting the host in and out of maintenance mode and shutting down and restarting the host.	Hosts
Host > **Configuration** > **Memory configuration**	Allows modifications to the host configuration.	Hosts
Host > **Configuration** > **Network configuration**	Allows configuration of network, firewall, and vMotion network.	Hosts
Host > **Configuration** > **Power**	Allows configuration of host power management settings.	Hosts
Host > **Configuration** > **Query patch**	Allows querying for installable patches and installing patches on the host.	Hosts
Host > **Configuration** > **Security profile and firewall**	Allows configuration of Internet services, such as SSH, Telnet, SNMP, and of the host firewall.	Hosts

Privilege Name	Description	Required On
Host > **Configuration** > **Storage partition configuration**	Allows VMFS datastore and diagnostic partition management. Users with this privilege can scan for new storage devices and manage iSCSI.	Hosts
Host > **Configuration** > **System Management**	Allows extensions to manipulate the file system on the host.	Hosts
Host > **Configuration** > **System resources**	Allows updates to the configuration of the system resource hierarchy.	Hosts
Host > **Configuration** > **Virtual machine autostart configuration**	Allows changes to the auto-start and auto-stop order of virtual machines on a single host.	Hosts

Host Inventory

Host inventory privileges control adding hosts to the inventory, adding hosts to clusters, and moving hosts in the inventory.

The table describes the privileges required to add and move hosts and clusters in the inventory.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 287: Host Inventory Privileges

Privilege Name	Description	Required On
Host > **Inventory** > **Add host to cluster**	Allows addition of a host to an existing cluster.	Clusters
Host > **Inventory** > **Add standalone host**	Allows addition of a standalone host.	Host folders
Host > **Inventory** > **Create cluster**	Allows creation of a new cluster.	Host folders
Host > **Inventory** > **Modify cluster**	Allows changing the properties of a cluster.	Clusters
Host > **Inventory** > **Move cluster or standalone host**	Allows moving a cluster or standalone host between folders. Privilege must be present at both the source and destination.	Clusters
Host > **Inventory** > **Move host**	Allows moving a set of existing hosts into or out of a cluster. Privilege must be present at both the source and destination.	Clusters
Host > **Inventory** > **Remove cluster**	Allows deletion of a cluster or standalone host. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Clusters, Hosts
Host > **Inventory** > **Remove host**	Allows removal of a host. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Hosts plus parent object
Host > **Inventory** > **Rename cluster**	Allows renaming a a cluster.	Clusters

Host Local Operations Privileges

Host local operations privileges control actions performed when the VMware Host Client is connected directly to a host.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 288: Host Local Operations Privileges

Privilege Name	Description	Required On
Host > **Local operations** > **Add host to vCenter**	Allows installation and removal of vCenter agents, such as vpxa and aam, on a host.	Root host
Host > **Local operations** > **Create virtual machine**	Allows creation of a new virtual machine from scratch on a disk without registering it on the host.	Root host
Host > **Local operations** > **Delete virtual machine**	Allows deletion of a virtual machine on disk. Supported for registered and unregistered virtual machines.	Root host
Host > **Local operations** > **Manage user groups**	Allows management of local accounts on a host.	Root host
Host > **Local operations** > **Reconfigure virtual machine**	Allows reconfiguring a virtual machine.	Root host

Host vSphere Replication Privileges

Host vSphere replication privileges control the use of virtual machine replication by VMware vCenter Site Recovery Manager™ for a host.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 289: Host vSphere Replication Privileges

Privilege Name	Description	Required On
Host > **vSphere Replication** > **Manage Replication**	Allows management of virtual machine replication on this host.	Hosts

Host Profile Privileges

Host Profile privileges control operations related to creating and modifying host profiles.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 290: Host Profile Privileges

Privilege Name	Description	Required On
Host profile > **Clear**	Allows clearing of profile related information.	Root vCenter Server
Host profile > **Create**	Allows creation of a host profile.	Root vCenter Server
Host profile > **Delete**	Allows deletion of a host profile.	Root vCenter Server

Privilege Name	Description	Required On
Host profile > **Edit**	Allows editing a host profile.	Root vCenter Server
Host profile > **Export**	Allows exporting a host profile	Root vCenter Server
Host profile > **View**	Allows viewing a host profile.	Root vCenter Server

vSphere with Tanzu Privileges

Namespaces privileges control who can create and manage VMware vSphere® with VMware Tanzu™ namespaces.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 291: Namespaces Privileges

Privilege Name	Description	Required On
	Allows for decommissioning operations of data stores.	Data stores
	Allows for backing up the contents of the etcd cluster (used only in VMware Cloud on AWS).	Clusters
Namespaces > **List Accessible Namespaces**	Allows listing the accessible namespaces.	Clusters
	Allows modifying the cluster-wide configuration, and enabling and disabling cluster namespaces.	Clusters
	Allows modifying the namespace self-service configuration.	Clusters (for activating and deactivating) Templates (for modifying the configuration) vCenter Server (for creating a template)
	Allows modifying namespace configuration options such as resource allocation and user permissions.	Clusters
	Allows manipulating the state of cluster capabilities (used internally only for VMware Cloud on AWS).	Clusters
	Allows initiation of the cluster upgrade.	Clusters

Network Privileges

Network privileges control tasks related to network management.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 292: Network Privileges

Privilege Name	Description	Required On
Network > **Assign network**	Allows assigning a network to a virtual machine.	Networks, Virtual Machines
Network > **Configure**	Allows configuring a network.	Networks, Virtual Machines
Network > **Move network**	Allows moving a network between folders. Privilege must be present at both the source and destination.	Networks
Network > **Remove**	Allows removal of a network. This privilege is deprecated. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Networks

Performance Privileges

Performance privileges control modifying performance statistics settings.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 293: Performance Privileges

Privilege Name	Description	Required On
Performance > **Modify intervals**	Allows creating, removing, and updating performance data collection intervals.	Root vCenter Server

Permissions Privileges

Permissions privileges control the assigning of roles and permissions.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 294: Permissions Privileges

Privilege Name	Description	Required On
Permissions > **Modify permission**	Allows defining one or more permission rules on an entity, or updating rules if rules are already present for the given user or group on the entity. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Any object plus parent object
Permissions > **Modify privilege**	Allows modifying a privilege's group or description. No vSphere Client user interface elements are associated with this privilege.	
Permissions > **Modify role**	Allows updating a role's name and the privileges that are associated with the role.	Any object
Permissions > **Reassign role permissions**	Allows reassigning all permissions of a role to another role.	Any object

Profile-driven Storage Privileges

Profile-driven storage privileges control operations related to storage profiles.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 295: Profile-driven Storage Privileges

Privilege Name	Description	Required On
Profile-driven storage > **Profile-driven storage update**	Allows changes to be made to storage profiles, such as creating and updating storage capabilities and virtual machine storage profiles.	Root vCenter Server
Profile-driven storage > **Profile-driven storage view**	Allows using and viewing defined storage capabilities and storage profiles.	Root vCenter Server

Resource Privileges

Resource privileges control the creation and management of resource pools, as well as the migration of virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 296: Resource Privileges

Privilege Name	Description	Required On
Resource > **Apply recommendation**	Allows accepting a suggestion by the server to perform a migration with vMotion.	Clusters
Resource > **Assign vApp to resource pool**	Allows assignment of a vApp to a resource pool.	Resource pools
Resource > **Assign virtual machine to resource pool**	Allows assignment of a virtual machine to a resource pool.	Resource pools
Resource > **Create resource pool**	Allows creation of resource pools.	Resource pools, clusters
Resource > **Migrate powered off virtual machine**	Allows migration of a powered off virtual machine to a different resource pool or host.	Virtual machines
Resource > **Migrate powered on virtual machine**	Allows migration with vMotion of a powered on virtual machine to a different resource pool or host.	
Resource > **Modify resource pool**	Allows changes to the allocations of a resource pool.	Resource pools
Resource > **Move resource pool**	Allows moving a resource pool. Privilege must be present at both the source and destination.	Resource pools
Resource > **Query vMotion**	Allows querying the general vMotion compatibility of a virtual machine with a set of hosts.	Root vCenter Server
Resource > **Remove resource pool**	Allows deletion of a resource pool. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Resource pools
Resource > **Rename resource pool**	Allows renaming of a resource pool.	Resource pools

Scheduled Task Privileges

Scheduled task privileges control creation, editing, and removal of scheduled tasks.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 297: Scheduled Task Privileges

Privilege Name	Description	Required On
Scheduled task > **Create tasks**	Allows scheduling of a task. Required in addition to the privileges to perform the scheduled action at the time of scheduling.	Any object
Scheduled task > **Modify task**	Allows reconfiguration of the scheduled task properties.	Any object
Scheduled task > **Remove task**	Allows removal of a scheduled task from the queue.	Any object
Scheduled task > **Run task**	Allows running the scheduled task immediately. Creating and running a scheduled task also requires permission to perform the associated action.	Any object

Sessions Privileges

Sessions privileges control the ability of extensions to open sessions on the vCenter Server system.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Note: Assign Sessions privileges only to administrators or trusted users.

Table 298: Session Privileges

Privilege Name	Description	Required On
Sessions > **Impersonate user**	Allows impersonation of another user. This capability is used by extensions.	Root vCenter Server
Sessions > **Message**	Allows setting of the global login message.	Root vCenter Server
Sessions > **Validate session**	Allows verification of session validity.	Root vCenter Server
Sessions > **View and stop sessions**	Allows viewing sessions and forcing log out of one or more logged-on users.	Root vCenter Server

Storage Views Privileges

Storage Views privileges control privileges for Storage Monitoring Service APIs.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 299: Storage Views Privileges

Privilege Name	Description	Required On
Storage views > **Configure service**	Allows privileged users to use all Storage Monitoring Service APIs. Use **Storage views** > **View** for privileges to read-only Storage Monitoring Service APIs.	Root vCenter Server
Storage views > **View**	Allows privileged users to use read-only Storage Monitoring Service APIs.	Root vCenter Server

Tasks Privileges

Tasks privileges control the ability of extensions to create and update tasks on the vCenter Server.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 300: Tasks Privileges

Privilege Name	Description	Required On
Tasks > **Create task**	Allows an extension to create a user-defined task. No vSphere Client user interface elements are associated with this privilege.	Root vCenter Server
Tasks > **Update task**	Allows an extension to update a user-defined task. No vSphere Client user interface elements are associated with this privilege.	Root vCenter Server

Transfer Service Privileges

Transfer service privileges are VMware internal. Do not use these privileges.

VcTrusts/VcIdentity Privileges

VcTrusts/VcIdentity privileges control access to various internal APIs and functionality related to trust between vCenter Server systems.

Table 301: VcTrusts/VcIdentity Privileges

Privilege Name	Description	Required On
VcTrusts/VcIdentity > **Create/Update/ Delete (Admin privs)**	Allows full administrative-level access to various internal APIs and functionality related to trust between vCenter Server systems.	N/A
VcTrusts/VcIdentity > **Create/Update/ Delete (below Admin privs)**	Allows reduced administrative access to various internal APIs and functionality related to trust between vCenter Server systems. This privilege restricts creating/updating/ deleting VcTrusts/VcIdentity so that the user cannot escalate non-administrator privileges.	N/A

Trusted Infrastructure Administrator Privileges

Trusted Infrastructure administrator privileges configure and manage a vSphere Trust Authority deployment.

These privileges determine who can perform configuration and management tasks for a vSphere Trust Authority deployment. See Prerequisites and Required Privileges for vSphere Trust Authority for more information about the Trust Authority roles and the TrustedAdmins group.

Table 302: Trusted Infrastructure Administrator Privileges

Privilege Name	Description	Required On
Trusted Infrastructure administrator > **Configure Key Server Trust**	Allows managing the Key Providers of the Key Provider Service.	Root vCenter Server
Trusted Infrastructure administrator > **Configure Trust Authority Host TPM certificates**	Allows creation and modification of the Attestation Service settings.	Root vCenter Server
Trusted Infrastructure administrator > **Configure Trust Authority Host metadata**	Allows editing the base images to be attested by the Attestation Service.	Root vCenter Server
Trusted Infrastructure administrator > **Configure attesting SSO**	Allows editing which hosts can be trusted by the Trust Authority Hosts.	Root vCenter Server
Trusted Infrastructure administrator > **Configure token conversion policy**	Allows configuring the token conversion policy.	Root vCenter Server
Trusted Infrastructure administrator > **List Trusted Infrastructure Hosts**	Allows reading information regarding the Trusted Hosts and the Trust Authority Hosts.	Root vCenter Server
Trusted Infrastructure administrator > **List information about the STS**	Allows exporting the Trusted Host details, so that they can be imported to the Trust Authority Cluster.	Root vCenter Server
Trusted Infrastructure administrator > **Manage Trusted Infrastructure Hosts**	Allows editing the information regarding the Trusted Hosts and the Trust Authority Hosts.	Root vCenter Server
Trusted Infrastructure administrator > **Read Key Server Trust**	Allows reading the Key Providers of the Key Provider Service.	Root vCenter Server
Trusted Infrastructure administrator > **Read attesting SSO**	Allows reading which hosts can be trusted by the Trust Authority Hosts.	Root vCenter Server
Trusted Infrastructure administrator > **Retrieve TPM Trust Authority Host certificates**	Allows reading the settings of the Attestation Service.	Root vCenter Server
Trusted Infrastructure administrator > **Retrieve Trust Authority Host metadatata**	Allows reading which base images can be attested by the Attestation Service.	Root vCenter Server

vApp Privileges

vApp privileges control operations related to deploying and configuring a vApp.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 303: vApp Privileges

Privilege Name	Description	Required On
vApp > **Add virtual machine**	Allows adding a virtual machine to a vApp.	vApps
vApp > **Assign resource pool**	Allows assigning a resource pool to a vApp.	vApps
vApp > **Assign vApp**	Allows assigning a vApp to another vApp	vApps
vApp > **Clone**	Allows cloning of a vApp.	vApps
vApp > **Create**	Allows creation of a vApp.	vApps
vApp > **Delete**	Allows deletion a vApp. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	vApps
vApp > **Export**	Allows export of a vApp from vSphere.	vApps
vApp > **Import**	Allows import of a vApp into vSphere.	vApps
vApp > **Move**	Allows moving a vApp to a new inventory location.	vApps
vApp > **Power Off**	Allows power off operations on a vApp.	vApps
vApp > **Power On**	Allows power on operations on a vApp.	vApps
vApp > **Rename**	Allows renaming a vApp.	vApps
vApp > **Suspend**	Allows suspension of a vApp.	vApps
vApp > **Unregister**	Allows unregistering a vApp. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	vApps
vApp > **View OVF Environment**	Allows viewing the OVF environment of a powered-on virtual machine within a vApp.	vApps
vApp > **vApp application configuration**	Allows modification of a vApp's internal structure, such as product information and properties.	vApps
vApp > **vApp instance configuration**	Allows modification of a vApp's instance configuration, such as policies.	vApps
vApp > **vApp managedBy configuration**	Allows an extension or solution to mark a vApp as being managed by that extension or solution. No vSphere Client user interface elements are associated with this privilege.	vApps
vApp > **vApp resource configuration**	Allows modification of a vApp's resource configuration. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	vApps

VcIdentityProviders Privileges

VcIdentityProviders privileges control access to the VcIdentityProviders API.

Table 304: VcIdentityProviders Privileges

Privilege Name	Description	Required On
VcIdentityProviders > **Create**	Allows create-only access to the VcIdentityProviders API (vCenter Server identity providers).	N/A
VcIdentityProviders > **Manage**	Allows administrative-level write access (create, read, update, delete) to the VcIdentityProviders API (vCenter Server identity providers).	N/A
VcIdentityProviders > **Read**	Allows read access to the VcIdentityProviders API (vCenter Server identity providers).	N/A

VMware vSphere Lifecycle Manager Configuration Privileges

VMware vSphere Lifecycle Manager configuration privileges control the ability to configure the vSphere Lifecycle Manager service.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Note: Assign privileges that authorize users to invoke VMware vSphere Lifecycle Manager APIs that accept URLs only to administrators or trusted users.

Table 305: VMware vSphere Lifecycle Manager Configuration Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Configure** > **Configure Service**	Allows configuring the vSphere Lifecycle Manager service and the scheduled patch download task.	Root vCenter Server

VMware vSphere Lifecycle Manager ESXi Health Perspectives Privileges

VMware vSphere Lifecycle ManagerESXi health perspective privileges control the ability to check the health of ESXi hosts and clusters.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 306: VMware vSphere Lifecycle Manager ESXi Health Perspectives Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **ESXi Health Perspectives** > **Read**	Allows querying the health of ESXi hosts and clusters.	Hosts Clusters
VMware vSphere Lifecycle Manager > **ESXi Health Perspectives** > **Write**	N/A	N/A

VMware vSphere Lifecycle Manager General Privileges

VMware vSphere Lifecycle Manager General privileges control the ability to read and write Lifecyle Manager resources.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 307: VMware vSphere Lifecycle Manager General Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Lifecycle Manager: General Privileges** > **Read**	Allows reading of the vSphere Lifecycle Manager resources. This privilege is required to get task information.	Root vCenter Server
VMware vSphere Lifecycle Manager > **Lifecycle Manager: General Privileges** > **Write**	Allows writing of the vSphere Lifecycle Manager resources. This privilege is required to cancel a vSphere Lifecycle Manager task.	Root vCenter Server

VMware vSphere Lifecycle Manager Hardware Compatibility Privileges

VMware vSphere Lifecycle Manager Hardware Compatibility privileges control the ability to discover and resolve potential hardware compatibility issues.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 308: VMware vSphere Lifecycle Manager Hardware Compatibility Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Hardware Compatibility Privileges** > **Access Hardware Compatibility**	Allows accessing the hardware compatibility data and resolving potential hardware compatibility issues.	Hosts

VMware vSphere Lifecycle Manager Image Privileges

VMware vSphere Lifecycle Manager Image privileges control the ability to manage images.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Note: Assign privileges that authorize users to invoke VMware vSphere Lifecycle Manager APIs that accept URLs only to administrators or trusted users.

Table 309: VMware vSphere Lifecycle Manager Image Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Image Privileges** > **Read**	Allows reading of vSphere Lifecycle Manager images. This privilege is required to: • List all the drafts for a cluster • Get more information on a draft • Perform a scan on a draft • Validate a draft • Retrieve the contents of a draft • Compute the effective component list • Get the contents of the current desired state document • Start a scan on a cluster • Get the compliance result • Get a recommendation • Export the current desired state as a depot, JSON file, or ISO	Root vCenter Server
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Image Privileges** > **Write**	Allows managing of vSphere Lifecycle Manager images. This privilege is required to: • Create, delete, or commit a draft • Import the desired state • Generate recommendations • Set or delete different portions of a draft	Root vCenter Server

VMware vSphere Lifecycle Manager Image Remediation Privileges

VMware vSphere Lifecycle Manager Image privileges control the ability to remediate images.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 310: VMware vSphere Lifecycle Manager Image Remediation Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Image Remediation Privileges** > **Read**	Allows performing the remediation pre-check.	Clusters
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Image Remediation Privileges** > **Write**	Allows performing the remediation.	Clusters

VMware vSphere Lifecycle Manager Settings Privileges

VMware vSphere Lifecycle Manager Settings privileges control the ability to manage depots and remediation policies.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Note: Assign privileges that authorize users to invoke VMware vSphere Lifecycle Manager APIs that accept URLs only to administrators or trusted users.

Table 311: VMware vSphere Lifecycle Manager Settings Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Settings Privileges** > **Read**	Allows reading of vSphere Lifecycle Manager depots and remediation policies.	Root vCenter Server
VMware vSphere Lifecycle Manager > **Lifecycle Manager: Settings Privileges** > **Write**	Allows writing of vSphere Lifecycle Manager depots and remediation policies.	Root vCenter Server

VMware vSphere Lifecycle Manager Manage Baseline Privileges

VMware vSphere Lifecycle Manager Manage Baseline privileges control the ability to manage baselines and baseline groups.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 312: VMware vSphere Lifecycle Manager Manage Baseline Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Manage Baseline** > **Attach Baseline**	Allows attaching baselines and baseline groups to objects in the vSphere inventory.	Root vCenter Server
VMware vSphere Lifecycle Manager > **Manage Baseline** > **Manage Baseline**	Allows creating, editing, or deleting baselines and baseline groups.	Root vCenter Server

VMware vSphere Lifecycle Manager Manage Patches and Upgrades Privileges

VMware vSphere Lifecycle Manager Manage Patches and Upgrades privileges control the ability to view, scan, and remediate applicable patches, extensions, or upgrades.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 313: VMware vSphere Lifecycle Manager Manage Patches and Upgrades Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Manage Patches and Upgrades** > **Remediate to Apply Patches, Extensions, and Upgrades**	Allows remediation of virtual machines and hosts to apply patches, extensions, or upgrades when you are using baselines. In addition, this privilege allows viewing the compliance status.	Root vCenter Server
VMware vSphere Lifecycle Manager > **Manage Patches and Upgrades** > **Scan for Applicable Patches, Extensions, and Upgrades**	Allows scanning virtual machines and hosts to search for applicable patches, extensions, or upgrades when you are using baselines.	Root vCenter Server
VMware vSphere Lifecycle Manager > **Manage Patches and Upgrades** > **Stage Patches and Extensions**	Allows staging patches or extensions to ESXi hosts when you are using baselines. In addition, this privilege allows viewing the compliance status of ESXi hosts.	Root vCenter Server
VMware vSphere Lifecycle Manager > **Manage Patches and Upgrades** > **View Compliance Status**	Allows viewing the baseline compliance information for an object in the vSphere inventory.	Root vCenter Server

VMware vSphere Lifecycle Manager Upload File Privileges

VMware vSphere Lifecycle Manager Upload File privileges control the ability to import updates to the vSphere Lifecycle Manager depot.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Note: Assign privileges that authorize users to invoke VMware vSphere Lifecycle Manager APIs that accept URLs only to administrators or trusted users.

Table 314: VMware vSphere Lifecycle Manager Upload File Privileges

Privilege Name	Description	Required On
VMware vSphere Lifecycle Manager > **Upload file** > **Upload file**	Allows uploading upgrade ISO and offline patch bundles.	Root vCenter Server

Virtual Machine Configuration Privileges

Virtual Machine Configuration privileges control the ability to configure virtual machine options and devices.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 315: Virtual Machine Configuration Privileges

Privilege Name	Description	Required On
Virtual machine > **Configuration** > **Acquire disk lease**	Allows disk lease operations for a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Add existing disk**	Allows adding an existing virtual disk to a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Add new disk**	Allows creation of a new virtual disk to add to a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Add or remove device**	Allows addition or removal of any non-disk device.	Virtual machines
Virtual machine > **Configuration** > **Advanced configuration**	Allows addition or modification of advanced parameters in the virtual machine's configuration file.	Virtual machines
Virtual machine > **Configuration** > **Change CPU count**	Allows changing the number of virtual CPUs.	Virtual machines
Virtual machine > **Configuration** > **Change Memory**	Allows changing the amount of memory allocated to the virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Change Settings**	Allows changing general virtual machine settings.	Virtual machines
Virtual machine > **Configuration** > **Change Swapfile placement**	Allows changing the swapfile placement policy for a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Change resource**	Allows changing the resource configuration of a set of virtual machine nodes in a given resource pool.	Virtual machines
Virtual machine > **Configuration** > **Configure Host USB device**	Allows attaching a host-based USB device to a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Configure Raw device**	Allows adding or removing a raw disk mapping or SCSI pass through device. Setting this parameter overrides any other privilege for modifying raw devices, including connection states.	Virtual machines
Virtual machine > **Configuration** > **Configure managedBy**	Allows an extension or solution to mark a virtual machine as being managed by that extension or solution.	Virtual machines
Virtual machine > **Configuration** > **Display connection settings**	Allows configuration of virtual machine remote console options.	Virtual machines
Virtual machine > **Configuration** > **Extend virtual disk**	Allows expansion of the size of a virtual disk.	Virtual machines
Virtual machine > **Configuration** > **Modify device settings**	Allows changing the properties of an existing device.	Virtual machines
Virtual machine > **Configuration** > **Query Fault Tolerance compatibility**	Allows checking if a virtual machine is compatible for Fault Tolerance.	Virtual machines
Virtual machine > **Configuration** > **Query unowned files**	Allows querying of unowned files.	Virtual machines

Privilege Name	Description	Required On
Virtual machine > **Configuration** > **Reload from path**	Allows changing a virtual machine configuration path while preserving the identity of the virtual machine. Solutions such as VMware vCenter Site Recovery Manager use this operation to maintain virtual machine identity during failover and failback.	Virtual machines
Virtual machine > **Configuration** > **Remove disk**	Allows removal of a virtual disk device.	Virtual machines
Virtual machine > **Configuration** > **Rename**	Allows renaming a virtual machine or modifying the associated notes of a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Reset guest information**	Allows editing the guest operating system information for a virtual machine.	Virtual machines
Virtual machine > **Configuration** > **Set annotation**	Allows adding or editing a virtual machine annotation.	Virtual machines
Virtual machine > **Configuration** > **Toggle disk change tracking**	Allows enabling or disabling of change tracking for the virtual machine's disks.	Virtual machines
Virtual machine > **Configuration** > **Toggle fork parent**	Allows enabling or disabling a vmfork parent.	Virtual machines
Virtual machine > **Configuration** > **Upgrade virtual machine compatibility**	Allows upgrade of the virtual machine’s virtual machine compatibility version.	Virtual machines

Virtual Machine Guest Operations Privileges

Virtual Machine Guest Operations privileges control the ability to interact with files and applications inside a virtual machine's guest operating system with the API.

See the *vSphere Web Services API Reference* documentation for more information on these operations.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 316: Virtual Machine Guest Operations

Privilege Name	Description	Effective on Object
Virtual machine > **Guest Operations** > **Guest Operation Alias modification**	Allows virtual machine guest operations that involve modifying the alias for the virtual machine.	Virtual machines
Virtual machine > **Guest Operations** > **Guest Operation Alias query**	Allows virtual machine guest operations that involve querying the alias for the virtual machine.	Virtual machines

Privilege Name	Description	Effective on Object
Virtual machine > **Guest Operations** > **Guest Operation Modifications**	Allows virtual machine guest operations that involve modifications to a guest operating system in a virtual machine, such as transferring a file to the virtual machine. No vSphere Client user interface elements are associated with this privilege.	Virtual machines
Virtual machine > **Guest Operations** > **Guest Operation Program Execution**	Allows virtual machine guest operations that involve running an application in the virtual machine. No vSphere Client user interface elements are associated with this privilege.	Virtual machines
Virtual machine > **Guest Operations** > **Guest Operation Queries**	Allows virtual machine guest operations that involve querying the guest operating system, such as listing files in the guest operating system. No vSphere Client user interface elements are associated with this privilege.	Virtual machines

Virtual Machine Interaction Privileges

Virtual Machine Interaction privileges control the ability to interact with a virtual machine console, configure media, perform power operations, and install VMware Tools.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 317: Virtual Machine Interaction

Privilege Name	Description	Required On
Virtual machine > **Interaction** > **Answer question**	Allows resolution of issues with virtual machine state transitions or runtime errors.	Virtual machines
Virtual machine > **Interaction** > **Backup operation on virtual machine**	Allows performance of backup operations on virtual machines.	Virtual machines
Virtual machine > **Interaction** > **Configure CD media**	Allows configuration of a virtual DVD or CD-ROM device.	Virtual machines
Virtual machine > **Interaction** > **Configure floppy media**	Allows configuration of a virtual floppy device.	Virtual machines
Virtual machine > **Interaction** > **Console interaction**	Allows interaction with the virtual machine's virtual mouse, keyboard, and screen.	Virtual machines

Privilege Name	Description	Required On
Virtual machine > **Interaction** > **Create screenshot**	Allows creation of a virtual machine screen shot.	Virtual machines
Virtual machine > **Interaction** > **Defragment all disks**	Allows defragment operations on all disks of the virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Device connection**	Allows changing the connected state of a virtual machine's disconnectable virtual devices.	Virtual machines
Virtual machine > **Interaction** > **Drag and Drop**	Allows drag and drop of files between a virtual machine and a remote client.	Virtual machines
Virtual machine > **Interaction** > **Guest operating system management by VIX API**	Allows management of the virtual machine's operating system through the VIX API.	Virtual machines
Virtual machine > **Interaction** > **Inject USB HID scan codes**	Allows injection of USB HID scan codes.	Virtual machines
Virtual machine > **Interaction** > **Pause or Unpause**	Allows pausing or unpausing of the virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Perform wipe or shrink operations**	Allows performing wipe or shrink operations on the virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Power Off**	Allows powering off a powered-on virtual machine. This operation powers down the guest operating system.	Virtual machines
Virtual machine > **Interaction** > **Power On**	Allows powering on a powered-off virtual machine, and resuming a suspended virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Record session on Virtual Machine**	Allows recording a session on a virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Replay session on Virtual Machine**	Allows replaying of a recorded session on a virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Reset**	Allows resetting of a virtual machine and reboots the guest operating system.	Virtual machines
Virtual machine > **Interaction** > **Resume Fault Tolerance**	Allows resuming of fault tolerance for a virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Suspend**	Allows suspending a powered-on virtual machine. This operation puts the guest in standby mode.	Virtual machines
Virtual machine > **Interaction** > **Suspend Fault Tolerance**	Allows suspension of fault tolerance for a virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Test failover**	Allows testing of Fault Tolerance failover by making the Secondary virtual machine the Primary virtual machine.	Virtual machines

Privilege Name	Description	Required On
Virtual machine > **Interaction** > **Test restart Secondary VM**	Allows termination of a Secondary virtual machine for a virtual machine using Fault Tolerance.	Virtual machines
Virtual machine > **Interaction** > **Turn Off Fault Tolerance**	Allows turning off Fault Tolerance for a virtual machine.	Virtual machines
Virtual machine > **Interaction** > **Turn On Fault Tolerance**	Allows turning on Fault Tolerance for a virtual machine.	Virtual machines
Virtual machine > **Interaction** > **VMware Tools install**	Allows mounting and unmounting the VMware Tools CD installer as a CD-ROM for the guest operating system.	Virtual machines

Virtual Machine Inventory Privileges

Virtual Machine Inventory privileges control adding, moving, and removing virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 318: Virtual Machine Inventory Privileges

Privilege Name	Description	Required On
Virtual machine > **Inventory** > **Create from existing**	Allows creation of a virtual machine based on an existing virtual machine or template, by cloning or deploying from a template.	Clusters, Hosts, Virtual machine folders
Virtual machine > **Inventory** > **Create new**	Allows creation of a virtual machine and allocation of resources for its execution.	Clusters, Hosts, Virtual machine folders
Virtual machine > **Inventory** > **Move**	Allows relocating a virtual machine in the hierarchy. The privilege must be present at both the source and destination.	Virtual machines
Virtual machine > **Inventory** > **Register**	Allows adding an existing virtual machine to a vCenter Server or host inventory.	Clusters, Hosts, Virtual machine folders
Virtual machine > **Inventory** > **Remove**	Allows deletion of a virtual machine. Deletion removes the virtual machine's underlying files from disk. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Virtual machines
Virtual machine > **Inventory** > **Unregister**	Allows unregistering a virtual machine from a vCenter Server or host inventory. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Virtual machines

Virtual Machine Provisioning Privileges

Virtual Machine Provisioning privileges control activities related to deploying and customizing virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 319: Virtual Machine Provisioning Privileges

Privilege Name	Description	Required On
Virtual machine > **Provisioning** > **Allow disk access**	Allows opening a disk on a virtual machine for random read and write access. Used mostly for remote disk mounting.	Virtual machines
Virtual machine > **Provisioning** > **Allow file access**	Allows operations on files associated with a virtual machine, including vmx, disks, logs, and nvram.	Virtual machines
Virtual machine > **Provisioning** > **Allow read-only disk access**	Allows opening a disk on a virtual machine for random read access. Used mostly for remote disk mounting.	Virtual machines
Virtual machine > **Provisioning** > **Allow virtual machine download**	Allows read operations on files associated with a virtual machine, including vmx, disks, logs, and nvram.	Root host or vCenter Server
Virtual machine > **Provisioning** > **Allow virtual machine files upload**	Allows write operations on files associated with a virtual machine, including vmx, disks, logs, and nvram.	Root host or vCenter Server
Virtual machine > **Provisioning** > **Clone template**	Allows cloning of a template.	Templates
Virtual machine > **Provisioning** > **Clone virtual machine**	Allows cloning of an existing virtual machine and allocation of resources.	Virtual machines
Virtual machine > **Provisioning** > **Create template from virtual machine**	Allows creation of a new template from a virtual machine.	Virtual machines
Virtual machine > **Provisioning** > **Customize**	Allows customization of a virtual machine's guest operating system without moving the virtual machine.	Virtual machines
Virtual machine > **Provisioning** > **Deploy template**	Allows deployment of a virtual machine from a template.	Templates
Virtual machine > **Provisioning** > **Mark as template**	Allows marking an existing powered off virtual machine as a template.	Virtual machines
Virtual machine > **Provisioning** > **Mark as virtual machine**	Allows marking an existing template as a virtual machine.	Templates
Virtual machine > **Provisioning** > **Modify customization specification**	Allows creation, modification, or deletion of customization specifications.	Root vCenter Server
Virtual machine > **Provisioning** > **Promote disks**	Allows promote operations on a virtual machine's disks.	Virtual machines
Virtual machine > **Provisioning** > **Read customization specifications**	Allows reading a customization specification.	Virtual machines

Virtual Machine Service Configuration Privileges

Virtual machine service configuration privileges control who can perform monitoring and management tasks on the service configuration.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 320: Virtual Machine Service Configuration Privileges

Privilege Name	Description
Virtual Machine > **Service configuration** > **Allow notifications**	Allows generating and consuming notification about service status.
Virtual Machine > **Service configuration** > **Allow polling of global event notifications**	Allows querying whether any notifications are present.
Virtual Machine > **Service configuration** > **Manage service configurations**	Allows creating, modifying, and deleting virtual machine services.
Virtual Machine > **Service configuration** > **Modify service configuration**	Allows modification of existing virtual machine service configuration.
Virtual Machine > **Service configuration** > **Query service configurations**	Allows retrieval of list of virtual machine services.
Virtual Machine > **Service configuration** > **Read service configuration**	Allows retrieval of existing virtual machine service configuration.

Virtual Machine Snapshot Management Privileges

Virtual machine snapshot management privileges control the ability to take, delete, rename, and restore snapshots.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 321: Virtual Machine State Privileges

Privilege Name	Description	Required On
Virtual machine > **Snapshot management** > **Create snapshot**	Allows creation of a snapshot from the virtual machine's current state.	Virtual machines
Virtual machine > **Snapshot management** > **Remove Snapshot**	Allows removal of a snapshot from the snapshot history.	Virtual machines
Virtual machine > **Snapshot management** > **Rename Snapshot**	Allows renaming a snapshot with a new name, a new description, or both.	Virtual machines
Virtual machine > **Snapshot management** > **Revert to snapshot**	Allows setting the virtual machine to the state it was in at a given snapshot.	Virtual machines

Virtual Machine vSphere Replication Privileges

Virtual Machine vSphere replication privileges control the use of replication by VMware vCenter Site Recovery Manager™ for virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 322: Virtual Machine vSphere Replication

Privilege Name	Description	Required On
Virtual machine > **vSphere Replication** > **Configure Replication**	Allows configuration of replication for the virtual machine.	Virtual machines
Virtual machine > **vSphere Replication** > **Manage Replication**	Allows triggering of full sync, online sync or offline sync on a replication.	Virtual machines
Virtual machine > **vSphere Replication** > **Monitor Replication**	Allows monitoring of replication.	Virtual machines

vServices Privileges

vServices privileges control the ability to create, configure, and update vService dependencies for virtual machines and vApps.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 323: vServices

Privilege Name	Description	Required On
vService > **Create dependency**	Allows creation of a vService dependency for a virtual machine or vApp.	vApps and virtual machines
vService > **Destroy dependency**	Allows removal of a vService dependency for a virtual machine or vApp.	vApps and virtual machines
vService > **Reconfigure dependency configuration**	Allows reconfiguration of a dependency to update the provider or binding.	vApps and virtual machines
vService > **Update dependency**	Allows updates of a dependence to configure the name or description.	vApps and virtual machines

vSphere Tagging Privileges

vSphere Tagging privileges control the ability to create and delete tags and tag categories, and assign and remove tags on vCenter Server inventory objects.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 324: vSphere Tagging Privileges

Privilege Name	Description	Required On
vSphere Tagging > **Assign or Unassign vSphere Tag**	Allows assignment or unassignment of a tag for an object in the vCenter Server inventory.	Any object
vSphere Tagging > **Assign or Unassign vSphere Tag on Object**	Allows objects to have tags assigned or unassigned. Use this privilege to limit which objects users are able to assign or unassign tags to.	Any object
vSphere Tagging > **Create vSphere Tag**	Allows creation of a tag.	Any object
vSphere Tagging > **Create vSphere Tag Category**	Allows creation of a tag category.	Any object
vSphere Tagging > **Delete vSphere Tag**	Allows deletion of a tag.	Any object
vSphere Tagging > **Delete vSphere Tag Category**	Allows deletion of a tag category.	Any object
vSphere Tagging > **Edit vSphere Tag**	Allows editing of a tag.	Any object
vSphere Tagging > **Edit vSphere Tag Category**	Allows editing of a tag category.	Any object
vSphere Tagging > **Modify UsedBy Field for Category**	Allows changing the UsedBy field for a tag category.	Any object
vSphere Tagging > **Modify UsedBy Field for Tag**	Allows changing the UsedBy field for a tag.	Any object

vSphere Client Privileges

vSphere Client privileges control offline access to vCenter Server.

These privileges apply to VMware Cloud only.

Understanding vSphere Hardening and Compliance

Organizations expect to keep their data secure by reducing the risk of data theft, cyberattack, or unauthorized access. Organizations also must often comply with one or more regulations from government standards to private standards, such as the National Institute of Standards and Technology (NIST) and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG). Ensuring that your vSphere environment is in compliance with such standards involves understanding a broader set of considerations including people, processes, and technology.

A high-level overview of security and compliance topics that require attention helps you plan your compliance strategy. You also benefit from other compliance-related resources on the VMware Web site.

Security Versus Compliance in the vSphere Environment

The terms security and compliance are often used interchangeably. However, they are unique and distinct concepts.

Security, often thought of as information security, is commonly defined as a set of technical, physical, and administrative controls that you implement to provide confidentiality, integrity, and availability. For example, you secure a host by locking down which accounts can log into it, and by what means (SSH, direct console, and so on). Compliance, by contrast, is a set of requirements necessary to meet the minimum controls established by different regulatory frameworks that provide limited guidance on any specific type of technology, vendor, or configuration. For example, the Payment Card Industry (PCI) has established security guidelines to help organizations proactively protect customer account data.

Security reduces the risk of data theft, cyberattack, or unauthorized access, while compliance is the proof that a security control is in place, typically within a defined time line. Security is primarily outlined in the design decisions and highlighted within the technology configurations. Compliance is focused on mapping the correlation between security controls and specific requirements. A compliance mapping provides a centralized view to list out many of the required security controls. Those controls are further detailed by including each security control's respective compliance citations as dictated by a domain such as NIST, PCI, FedRAMP, HIPAA, and so forth.

Effective cybersecurity and compliance programs are built on three pillars: people, process, and technology. A general misconception is that technology alone can solve all your cybersecurity needs. Technology does play a large and important role in the development and execution of an information security program. However, technology without process and procedures, awareness and training, creates a vulnerability within your organization.

When defining your security and compliance strategies, keep the following in mind:

- People need general awareness and training, whereas IT staff need specific training.
- Process defines how your organization's activities, roles, and documentation are used to mitigate risk. Processes are only effective if people follow them correctly.
- Technology can be used to prevent or reduce the impact of cybersecurity risk to your organization. Which technology to use depends on your organization's risk acceptance level.

VMware provides Compliance Kits that contain both an Audit Guide and a Product Applicability Guide, helping to bridge the gap between compliance and regulatory requirements and implementation guides. For more information, see https://core.vmware.com/compliance.

Glossary of Compliance Terms

Compliance introduces specific terms and definitions that are important to understand.

Table 325: Compliance Terms

Term	Definition
CJIS	Criminal Justice Information Services. In the context of compliance, the CJIS produces a Security Policy for how local, state, and federal criminal justice and law enforcement agencies must take security precautions to protect sensitive information such as fingerprints and criminal backgrounds.
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guide. The Defense Information Systems Agency (DISA) is the entity responsible for maintaining the security posture of the Department of Defense (DoD) IT infrastructure. DISA accomplishes this task by developing and using Security Technical Implementation Guides, or "STIGs."
FedRAMP	Federal Risk and Authorization Management Program. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
HIPAA	Health Insurance Portability and Accountability Act. Passed by Congress in 1996, HIPAA does the following: • Gives millions of American workers and their families the ability to transfer and continue health insurance coverage for when they change or lose jobs • Reduces health care fraud and abuse • Mandates industry-wide standards for health care information on electronic billing and other processes

Term	Definition
	• Requires the protection and confidential handling of protected health information The latter bullet is of most importance to *vSphere Security* documentation.
NCCoE	National Cybersecurity Center of Excellence. NCCoE is a U.S government organization that produces and publicly shares solutions to cybersecurity problems that U.S. businesses encounter. The center forms a team of people from cybersecurity technology companies, other federal agencies, and academia to address each problem.
NIST	National Institute of Standards and Technology. Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to advocate for U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that increase economic security and improve our quality of life.
PAG	Product Applicability Guide. A document that provides general guidance for organizations that are considering a company's solutions to help them address compliance requirements.
PCI DSS	Payment Card Industry Data Security Standard. A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
VVD/VCF Compliance Solutions	VMware Validated Design/VMware Cloud Foundation. The VMware Validated Designs provide comprehensive and extensively tested blueprints to build and operate a Software-Defined Data Center. VVD/VCF compliance solutions enable customers to meet compliance requirements for multiple government and industry regulations.

Understanding the vSphere Security Configuration Guide

VMware creates Security Hardening Guides that provide prescriptive guidance about deploying and operating VMware products in a secure manner. For vSphere, this guide is called the *vSphere Security Configuration Guide* (formerly known as the *Hardening Guide*).

The *vSphere Security Configuration Guide* contains security best practices for vSphere. The *vSphere Security Configuration Guide* does not map directly to regulatory guidelines or frameworks, and so is not a compliance guide. Also, the *vSphere Security Configuration Guide* is not intended for use as a security checklist. Security is always a tradeoff. When you implement security controls, you might affect usability, performance, or other operational tasks negatively. Consider your workloads, usage patterns, organizational structure, and so on carefully before making security changes, whether the advice is from VMware or from other industry sources. If your organization is subject to regulatory compliance needs, see Security Versus Compliance in the vSphere Environment or visit https://core.vmware.com/compliance. This site features compliance kits and product audit guides to help vSphere administrators and regulatory auditors secure and attest virtual infrastructure for regulatory frameworks, such as NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001, and more.

The *vSphere Security Configuration Guide* does not discuss securing the following items:

- Software running inside the virtual machine, such as the Guest OS and applications
- Traffic running through the virtual machine networks
- Security of add-on products

The *vSphere Security Configuration Guide* is not meant to be used as a "compliance" tool. The *vSphere Security Configuration Guide* does enable you to take initial steps towards compliance, but used by itself, it does not ensure that your deployment is compliant. For more information about compliance, see Security Versus Compliance in the vSphere Environment.

Reading the vSphere Security Configuration Guide

The *vSphere Security Configuration Guide* is a spreadsheet that contains security-related guidelines to assist you with modifying your vSphere security configuration. These guidelines are group into tabs based on the affected components, with some or all of the following columns.

Table 326: vSphere Security Configuration Guide Spreadsheet Columns

Column Heading	Description
Guideline ID	A unique two-part ID to reference a security configuration or hardening recommendation. The first part indicates the component, defined as follows: • ESXi: ESXi hosts • VM: Virtual machines • vNetwork: Virtual switches
Description	A short explanation of the particular recommendation.
Discussion	Description of the vulnerability behind a particular recommendation.
Configuration Parameter	Provides the applicable configuration parameter or filename, if any.
Desired Value	The desired state or value of the recommendation. Possible values include: • N/A • Site Specific • False • True • Enabled • Disabled • Not present or False
Default Value	The default value set by vSphere.
Is desired value the default?	States if the security setting is the default product configuration.
Action Needed	The type of action to take on the particular recommendation. Actions include: • Update • Audit Only • Modify • Add • Remove
Setting Location in the vSphere Client	Steps for checking on the value by using the vSphere Client.
Negative Functional Impact in Change From Default?	Description, if any, of a potential negative impact from using the security recommendation.
PowerCLI Command Assessment	Steps for checking on the value by using PowerCLI.
PowerCLI Command Remediation Example	Steps for setting (remediating) the value by using PowerCLI.
vCLI Command Remediation	Steps for setting (remediating) the value by using the vCLI commands.
PowerCLI Command Assessment	Steps for checking on the value by using the PowerCLI commands.
PowerCLI Command Remediation	Steps for setting (remediating) the value by using the PowerCLI commands.
Able to set using Host Profile	Whether the setting can be accomplished by using Host Profiles (applies only to ESXi guidelines).

Column Heading	Description
Hardening	If TRUE, then the guideline has only one implementation to be compliant. If FALSE then you can satisfy the guideline implementation by more than one configuration setting. The actual setting is often site-specific.
Site Specific Setting	If TRUE, then the setting to be compliant with the guideline depends on rules or standards that are specific to that vSphere deployment.
Audit Setting	If TRUE, then the value of the listed setting might need to be modified to satisfy site-specific rules.

Note: These columns might change over time as required. For example, recent additions include the DISA STIG ID, Hardening, and Site Specific Setting columns. Check https://blogs.vmware.com for announcements about updates to the *vSphere Secure Configuration Guide*.

Do not blindly apply guidelines in the *vSphere Secure Configuration Guide* to your environment. Rather, take time to evaluate each setting and make an informed decision whether you want to apply it. At a minimum, you can use the instructions in the Assessment columns to verify the security of your deployment.

The *vSphere Secure Configuration Guide* is an aid to begin implementing compliance in your deployment. When used with the Defense Information Systems Agency (DISA) and other compliance guidelines, the *vSphere Secure Configuration Guide* enables you to map vSphere security controls to the compliance flavor per each guideline.

About the National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is a non-regulatory government agency that develops technology, metrics, standards, and guidelines. Compliance with NIST standards and guidelines has become a top priority in many industries today.

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations, from nanoscale devices, up to earthquake-resistant skyscrapers and global communication networks.

The Federal Information Security Management Act (FISMA) is a United States federal law passed in 2002 that made it a requirement for federal agencies to develop, document, and implement an information security and protection program. NIST plays an important role in the FISMA implementation by producing key security standards and guidelines (for example, FIPS 199, FIPS 200, and SP 800 series).

Government and private organizations use NIST 800-53 to secure information systems. Cybersecurity and privacy controls are essential to protect organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals from a diverse set of threats. Some of these threats include hostile cyber-attacks, natural disasters, structural failures, and human errors. VMware has enlisted a third-party audit partner to evaluate VMware products and solutions against the NIST 800-53 catalog of controls. For more information, visit the NIST webpage at https://www.nist.gov/cyberframework.

About DISA STIGs

The Defense Information Systems Agency (DISA) develops and publishes Security Technical Implementation Guides, or "STIGs." DISA STIGs provide technical guidance for hardening systems and reducing threats.

The Defense Information Systems Agency (DISA) is the U.S. Department of Defense (DoD) combat support agency responsible for maintaining the security posture of the DOD Information Network (DODIN). One of the ways DISA accomplishes this task is by developing, disseminating, and mandating the implementation of Security Technical Implementation Guides, or STIGs. In brief, STIGs are portable, standards-based guides for hardening systems. STIGs are mandatory for U.S. DoD IT systems and, as such, provide a vetted, secure baseline for non-DoD entities to measure their security posture.

Vendors such as VMware submit suggested security hardening guidance to DISA for evaluation, based on DISA protocols and feedback. Once that process is complete, the official STIG is published on the DISA organization's web site at https://public.cyber.mil/stigs/. VMware provides security baselines and hardening guidance for vSphere as part of the *vSphere Security Configuration Guide*. See https://core.vmware.com/security.

About VMware Security Development Lifecycle

The VMware Security Development Lifecycle (SDL) program identifies and mitigates security risk during the development phase of VMware software products. VMware also operates the VMware Security Response Center (VSRC) to conduct the analysis and remediation of software security issues in VMware products.

The SDL is the software development methodology that the VMware Security Engineering, Communication, and Response (vSECR) group, and VMware product development groups, use to help identify and mitigate security issues. For more information about the VMware Security Development Lifecycle, see the webpage at https://www.vmware.com/security/sdl.html.

The VSRC works with customers and the security research community to achieve the goals of addressing security issues and providing customers with actionable security information in a timely manner. For more information about the VMware Security Response Center, see the webpage at https://www.vmware.com/security/vsrc.html.

Audit Logging

Audit logging of network traffic, compliance alerts, firewall activity, operating system changes, and provisioning activities is considered a best practice for maintaining the security of any IT environment. In addition, logging is a specific requirement of many regulations and standards.

One of the first steps to take for ensuring you are aware of changes to your infrastructure is to audit your environment. By default, vSphere includes tools that enable you to view and track changes. For example, you can use the Tasks and Events tab in the vSphere Client on any object in your vSphere hierarchy to see what changes have occurred. You can also use the PowerCLI to retrieve events and tasks. Also, vRealize Log Insight offers audit logging to support collection and retention of important system events. In addition, many third-party tools are available that provide vCenter auditing.

Log files can provide an audit trail to help determine who or what is accessing a host, a virtual machine, and so on. For more information, see ESXi Log File Locations.

Single Sign-On Audit Events

Single Sign-On (SSO) audit events are records of user or system actions for accessing the SSO services.

vCenter Server 6.7 Update 2 and later improves VMware vCenter Single Sign-On auditing by adding events for the following operations:

- User management
- Login
- Group creation
- Identity source
- Policy updates

The supported identity sources are vsphere.local, Integrated Windows Authentication (IWA), and Active Directory over LDAP.

When a user logs in to vCenter Server through Single Sign-On, or makes changes that affect SSO, the following audit events are written to the SSO audit log file:

- **Login and Logout Attempts:** Events for all the successful and failed login and logout operations.

- **Privilege Change:** Event for change in a user role or permissions.
- **Account Change:** Event for change in the user account information, for example, user name, password, or any additional account information.
- **Security Change:** Event for change in a security configuration, parameter, or policy.
- **Account Enabled or Disabled:** Event for when an account is enabled or disabled.
- **Identity Source:** Event for adding, deleting, or editing an identity source.

In the vSphere Client, event data is displayed in the **Monitor** tab. See the *vSphere Monitoring and Performance* documentation.

SSO audit event data includes the following details:

- Timestamp of when the event occurred.
- User who performed the action.
- Description of the event.
- Severity of the event.
- IP address of client used to connect to vCenter Server, if available.

SSO Audit Event Log Overview

The vSphere Single-Sign On process writes audit events to the `audit_events.log` file in the `/var/log/audit/sso-events/` directory.

CAUTION: Never manually edit the `audit_events.log` file, as doing so might cause the audit logging to fail.

Keep the following in mind when working with the `audit_events.log` file:

- The log file is archived once it reaches 50 MB.
- A maximum of 10 archive files is kept. If the limit is reached, the oldest file is purged when a new archive is created.
- The archive files are named `audit_events-<index>.log.gz`, where the index is a numeral from 1 to 10. The first archive created is index 1, and is increased with each subsequent archive.
- The oldest events are in archive index 1. The highest indexed file is the latest archive.

Understanding Security and Compliance Next Steps

Conducting a security assessment is the first step in understanding any vulnerabilities in your infrastructure. A security assessment is part of a security audit, which looks at both systems and practices, including security compliance.

A security assessment generally refers to scanning your organization's physical infrastructure (firewalls, networks, hardware, and so on) to identify vulnerabilities and flaws. A security assessment is not the same as a security audit. A security audit includes not only a review of physical infrastructure but other areas such as policy and standard operating procedures, including security compliance. After you have the audit, you can decide on the steps to remedy the problems within the system.

You might ask these general questions when preparing to conduct a security audit:

1. Is our organization mandated to adhere to a compliance regulation? If so which one(s)?
2. What is our audit interval?
3. What is our internal self-assessment interval?
4. Do we have access to previous audit results and have we viewed them?
5. Do we use a third-party audit firm to help us prepare for an audit? If so, what is their level of comfort with virtualization?
6. Do we run vulnerability scans against the systems and applications? When and how often?
7. What are our internal cybersecurity policies?
8. Is your audit logging configured according to your needs? See Audit Logging.

In the absence of specific guidance or direction on where to begin, you can jumpstart securing your vSphere environment by:

- Keeping your environment up-to-date with the latest software and firmware patches
- Maintaining good password management and hygiene for all accounts
- Reviewing vendor-approved security recommendations
- Referring to the VMware Security Configuration Guides (see Understanding the vSphere Security Configuration Guide)
- Using readily available and proven guidance from policy frameworks such as NIST, ISO, and so forth
- Following guidance from regulatory compliance frameworks such as PCI, DISA, and FedRAMP

vCenter Server and FIPS

In vSphere 7.0 Update 2 and later, you can enable FIPS-validated cryptography on the vCenter Server Appliance.

FIPS 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. vSphere uses FIPS-validated cryptographic modules to match those specified by the FIPS 140-2 standard. The goal of vSphere FIPS support is to ease the compliance and security activities in various regulated environments.

In vSphere 6.7 and later, ESXi and vCenter Server use FIPS-validated cryptography to protect management interfaces and the VMware Certificate Authority (VMCA).

vSphere 7.0 Update 2 and later adds additional FIPS-validated cryptography to vCenter Server Appliance. By default, this FIPS validation option is disabled.

Note: vSphere favors compatibility over FIPS, so some components have considerations to be aware of. See Considerations When Using FIPS.

FIPS Modules

A cryptographic module is a set of hardware, software, or firmware that implements security functions. ESXi uses several FIPS 140-2 validated cryptographic modules.

The following table shows the set of FIPS 140-2 validated cryptographic modules in use by ESXi.

Table 327: FIPS Modules

Cryptographic Module	Security Policy Version	Algorithms (CAVP)	Cryptographic Module Validation Program
Vmkernel Cryptographic Module	1.0	AES, SHS, DRBG, HMAC (C 1172)	Certificate #3073
Vmkernel Cryptographic Module Loader	Not applicable	HMAC, SHS (C 1171)	Certificate #3073
Vmkernel DRBG Cryptographic Module	Not applicable	AES, DRBG (C 499)	NA
VMware OpenSSL FIPS Object Module	2.0.20-vmw	DRBG, AES, SHS, HMAC, DSA, RSA, ECDSA, KAS-FFC, KAS-ECC (C 470)	Certificate #3550 and #3857

Enable and Disable FIPS on the vCenter Server Appliance

You can enable or disable FIPS-validated cryptography on the vCenter Server Appliance by using HTTP requests.

You can use various ways to execute HTTP requests. This task shows how to use the Developer Center in the vSphere Client to enable and disable FIPS on the vCenter Server Appliance. See *VMware vCenter Server Management Programming Guide* for more information about using APIs to work with the vCenter Server Appliance.

1. Log in to the vCenter Server system with the vSphere Client.
2. From the Menu, select **Developer Center**.
3. Click **API Explorer**.
4. From the **Select API** drop-down menu, select **appliance**.
5. Scroll down through the categories and expand **system/security/global_fips**.
6. Expand **GET** and click **Execute** under **Try it out**.
   You can view the current setting under **Response**.
7. Change the setting.
   a) To enable FIPS, expand **PUT**, enter the following in the `request_body` , and click **Execute**.

```
{
"enabled":true
}
```

   b) To disable FIPS, expand **PUT**, enter the following in the `request_body` , and click **Execute**.

```
{
"enabled":false
}
```

The vCenter Server Appliance reboots after you enable or disable FIPS.

Considerations When Using FIPS

When enabling FIPS on vCenter Server Appliance, some components present functional constraints currently.

You should see no differences after enabling FIPS on vCenter Server, however there are some considerations to be aware of.

Table 328: FIPS Considerations

Product or Component	Consideration	Workaround
vSphere Single Sign-On	When you enable FIPS, vCenter Server supports only cryptographic modules for federated authentication. As a result, RSA SecureID and some CAC cards no longer function.	Use federated authentication. See the *vSphere Authentication* documentation for details.
Non-VMware and partner vSphere Client UI plug-ins	These plug-ins might not work with FIPS enabled.	Upgrade plug-ins to use conformant encryption libraries. See "Preparing Local Plug-ins for FIPS Compliance" at https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance.

Product or Component	Consideration	Workaround
vCenter Server file-based backup and restore mechanism	File-based backup and restore with SMB is not FIPS compliant.	Use a different protocol for backup and restore (FTP, FTPS, HTTP, HTTPS, SFTP, or NFS).

vSphere Resource Management

vSphere Resource Management describes resource management for VMware®ESXi and vCenter® Server environments.

This documentation focuses on the following topics.

- Resource allocation and resource management concepts
- Virtual machine attributes and admission control
- Resource pools and how to manage them
- Clusters, vSphere® Distributed Resource Scheduler (DRS), vSphere Distributed Power Management (DPM), and how to work with them
- Datastore clusters, Storage DRS, Storage I/O Control, and how to work with them
- Advanced resource management options
- Performance considerations

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

This information is for system administrators who want to understand how the system manages resources and how they can customize the default behavior. It's also essential for anyone who wants to understand and use resource pools, clusters, DRS, datastore clusters, Storage DRS, Storage I/O Control, or vSphere DPM.

This documentation assumes you have a working knowledge of VMware ESXi and of vCenter Server.

Note: In this document, "Memory" can refer to physical RAM or Persistent Memory.

Getting Started with Resource Management

To understand resource management, you must be aware of its components, its goals, and how best to implement it in a cluster setting.

Resource allocation settings for a virtual machine (shares, reservation, and limit) are discussed, including how to set them and how to view them. Also, admission control, the process whereby resource allocation settings are validated against existing resources is explained.

Resource management is the allocation of resources from resource providers to resource consumers.

The need for resource management arises from the overcommitment of resources—that is, more demand than capacity and from the fact that demand and capacity vary over time. Resource management allows you to dynamically reallocate resources, so that you can more efficiently use available capacity.

Note: In this chapter, "Memory" refers to physical RAM.

Resource Types

Resources include CPU, memory, power, storage, and network resources.

Note: ESXi manages network bandwidth and disk resources on a per-host basis, using network traffic shaping and a proportional share mechanism, respectively.

Resource Providers

Hosts and clusters, including datastore clusters, are providers of physical resources.

For hosts, available resources are the host's hardware specification, minus the resources used by the virtualization software.

A cluster is a group of hosts. You can create a cluster using vSphere Client, and add multiple hosts to the cluster. vCenter Server manages these hosts' resources jointly: the cluster owns all of the CPU and memory of all hosts. You can enable the cluster for joint load balancing or failover. See Creating a DRS Cluster for more information.

A datastore cluster is a group of datastores. Like DRS clusters, you can create a datastore cluster using the vSphere Client, and add multiple datastores to the cluster. vCenter Server manages the datastore resources jointly. You can enable Storage DRS to balance I/O load and space utilization. See Creating a Datastore Cluster.

Resource Consumers

Virtual machines are resource consumers.

The default resource settings assigned during creation work well for most machines. You can later edit the virtual machine settings to allocate a share-based percentage of the total CPU, memory, and storage I/O of the resource provider or a guaranteed reservation of CPU and memory. When you power on that virtual machine, the server checks whether enough unreserved resources are available and allows power on only if there are enough resources. This process is called admission control.

A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. Accordingly, resource pools can be considered both resource providers and consumers. They provide resources to child resource pools and virtual machines, but are also resource consumers because they consume their parents' resources. See Managing Resource Pools.

ESXi hosts allocate each virtual machine a portion of the underlying hardware resources based on a number of factors:

- Resource limits defined by the user.
- Total available resources for the ESXi host (or the cluster).
- Number of virtual machines powered on and resource usage by those virtual machines.
- Overhead required to manage the virtualization.

Goals of Resource Management

When managing your resources, you must be aware of what your goals are.

In addition to resolving resource overcommitment, resource management can help you accomplish the following:

- Performance Isolation: Prevent virtual machines from monopolizing resources and guarantee predictable service rates.
- Efficient Usage: Exploit undercommitted resources and overcommit with graceful degradation.
- Easy Administration: Control the relative importance of virtual machines, provide flexible dynamic partitioning, and meet absolute service-level agreements.

Configuring Resource Allocation Settings

When available resource capacity does not meet the demands of the resource consumers (and virtualization overhead), administrators might need to customize the amount of resources that are allocated to virtual machines or to the resource pools in which they reside.

Use the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine. In particular, administrators have several options for allocating resources.

- Reserve the physical resources of the host or cluster.

- Set an upper bound on the resources that can be allocated to a virtual machine.
- Guarantee that a particular virtual machine is always allocated a higher percentage of the physical resources than other virtual machines.

Note: In this chapter, "Memory" refers to physical RAM.

Resource Allocation Shares

Shares specify the relative importance of a virtual machine (or resource pool). If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources.

Shares are typically specified as **High**, **Normal**, or **Low** and these values specify share values with a 4:2:1 ratio, respectively. You can also select **Custom** to assign a specific number of shares (which expresses a proportional weight) to each virtual machine.

Specifying shares makes sense only with regard to sibling virtual machines or resource pools, that is, virtual machines or resource pools with the same parent in the resource pool hierarchy. Siblings share resources according to their relative share values, bounded by the reservation and limit. When you assign shares to a virtual machine, you always specify the priority for that virtual machine relative to other powered-on virtual machines.

The following table shows the default CPU and memory share values for a virtual machine. For resource pools, the default CPU and memory share values are the same, but must be multiplied as if the resource pool were a virtual machine with four virtual CPUs and 16 GB of memory.

Table 329: Share Values

Setting	CPU share values	Memory share values
High	2000 shares per virtual CPU	20 shares per megabyte of configured virtual machine memory.
Normal	1000 shares per virtual CPU	10 shares per megabyte of configured virtual machine memory.
Low	500 shares per virtual CPU	5 shares per megabyte of configured virtual machine memory.

For example, an SMP virtual machine with two virtual CPUs and 1GB RAM with CPU and memory shares set to **Normal** has 2x1000=2000 shares of CPU and 10x1024=10240 shares of memory.

Virtual machines with more than one virtual CPU are called SMP (symmetric multiprocessing) virtual machines.

The relative priority represented by each share changes when a new virtual machine is powered on. This affects all virtual machines in the same resource pool. All of the virtual machines have the same number of virtual CPUs. Consider the following examples.

- Two CPU-bound virtual machines run on a host with 8GHz of aggregate CPU capacity. Their CPU shares are set to **Normal** and get 4GHz each.
- A third CPU-bound virtual machine is powered on. Its CPU shares value is set to **High**, which means it should have twice as many shares as the machines set to **Normal**. The new virtual machine receives 4GHz and the two other machines get only 2GHz each. The same result occurs if the user specifies a custom share value of 2000 for the third virtual machine.

Resource Allocation Reservation

A reservation specifies the guaranteed minimum allocation for a virtual machine.

vCenter Server or ESXi allows you to power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine. The server guarantees that amount even when the physical server is heavily loaded. The reservation is expressed in concrete units (megahertz or megabytes).

For example, assume you have 2GHz available and specify a reservation of 1GHz for VM1 and 1GHz for VM2. Now each virtual machine is guaranteed to get 1GHz if it needs it. However, if VM1 is using only 500MHz, VM2 can use 1.5GHz.

Reservation defaults to 0. You can specify a reservation if you need to guarantee that the minimum required amounts of CPU or memory are always available for the virtual machine.

Resource Allocation Limit

Limit specifies an upper bound for CPU, memory, or storage I/O resources that can be allocated to a virtual machine.

A server can allocate more than the reservation to a virtual machine, but never allocates more than the limit, even if there are unused resources on the system. The limit is expressed in concrete units (megahertz, megabytes, or I/O operations per second).

CPU, memory, and storage I/O resource limits default to unlimited. When the memory limit is unlimited, the amount of memory configured for the virtual machine when it was created becomes its effective limit.

In most cases, it is not necessary to specify a limit. There are benefits and drawbacks:

- Benefits — Assigning a limit is useful if you start with a small number of virtual machines and want to manage user expectations. Performance deteriorates as you add more virtual machines. You can simulate having fewer resources available by specifying a limit.
- Drawbacks — You might waste idle resources if you specify a limit. The system does not allow virtual machines to use more resources than the limit, even when the system is underutilized and idle resources are available. Specify the limit only if you have good reasons for doing so.

Resource Allocation Settings Suggestions

Select resource allocation settings (reservation, limit and shares) that are appropriate for your ESXi environment.

The following guidelines can help you achieve better performance for your virtual machines.

- Use **Reservation** to specify the minimum acceptable amount of CPU or memory, not the amount you want to have available. The amount of concrete resources represented by a reservation does not change when you change the environment, such as by adding or removing virtual machines. The host assigns additional resources as available based on the limit for your virtual machine, the number of shares and estimated demand.
- When specifying the reservations for virtual machines, do not commit all resources (plan to leave at least 10% unreserved). As you move closer to fully reserving all capacity in the system, it becomes increasingly difficult to make changes to reservations and to the resource pool hierarchy without violating admission control. In a DRS-enabled cluster, reservations that fully commit the capacity of the cluster or of individual hosts in the cluster can prevent DRS from migrating virtual machines between hosts.
- If you expect frequent changes to the total available resources, use **Shares** to allocate resources fairly across virtual machines. If you use **Shares**, and you upgrade the host, for example, each virtual machine stays at the same priority (keeps the same number of shares) even though each share represents a larger amount of memory, CPU, or storage I/O resources.

Edit Settings

Use the Edit Settings dialog box to change allocations for memory and CPU resources.

1. Browse to the virtual machine in the vSphere Client.
2. Right-click and select **Edit Settings**.
3. Edit the CPU Resources.

Option	Description
Shares	CPU shares for this resource pool with respect to the parent's total. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each virtual machine a specific number of shares, which expresses a proportional weight.
Reservation	Guaranteed CPU allocation for this resource pool.
Limit	Upper limit for this resource pool's CPU allocation. Select **Unlimited** to specify no upper limit.

4. Edit the Memory Resources.

Option	Description
Shares	Memory shares for this resource pool with respect to the parent's total. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each virtual machine a specific number of shares, which expresses a proportional weight.
Reservation	Guaranteed memory allocation for this resource pool.
Limit	Upper limit for this resource pool's memory allocation. Select **Unlimited** to specify no upper limit.

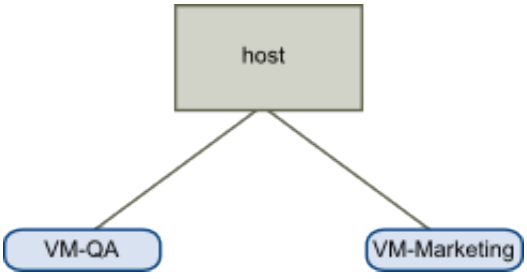
5. Click **OK**.

Changing Resource Allocation Settings—Example

The following example illustrates how you can change resource allocation settings to improve virtual machine performance.

Assume that on an ESXi host, you have created two new virtual machines—one each for your QA (VM-QA) and Marketing (VM-Marketing) departments.

Figure 96: Single Host with Two Virtual Machines



In the following example, assume that VM-QA is memory intensive and accordingly you want to change the resource allocation settings for the two virtual machines to:

- Specify that, when system memory is overcommitted, VM-QA can use twice as much CPU and memory resources as the Marketing virtual machine. Set the CPU shares and memory shares for VM-QA to **High** and for VM-Marketing set them to **Normal**.
- Ensure that the Marketing virtual machine has a certain amount of guaranteed CPU resources. You can do so using a reservation setting.

1. Browse to the virtual machines in the vSphere Client.
2. Right-click **VM-QA**, the virtual machine for which you want to change shares, and select **Edit Settings**.
3. Under **Virtual Hardware**, expand CPU and select **High** from the **Shares** drop-down menu.
4. Under **Virtual Hardware**, expand Memory and select **High** from the **Shares** drop-down menu.
5. Click **OK**.
6. Right-click the marketing virtual machine (**VM-Marketing**) and select **Edit Settings**.
7. Under **Virtual Hardware**, expand CPU and change the **Reservation** value to the desired number.
8. Click **OK**.

Admission Control

When you power on a virtual machine, the system checks the amount of CPU and memory resources that have not yet been reserved. Based on the available unreserved resources, the system determines whether it can guarantee the reservation for which the virtual machine is configured (if any). This process is called admission control.

If enough unreserved CPU and memory are available, or if there is no reservation, the virtual machine is powered on. Otherwise, an `Insufficient Resources` warning appears.

Note: In addition to the user-specified memory reservation, for each virtual machine there is also an amount of overhead memory. This extra memory commitment is included in the admission control calculation.

When the vSphere DPM feature is enabled, hosts might be placed in standby mode (that is, powered off) to reduce power consumption. The unreserved resources provided by these hosts are considered available for admission control. If a virtual machine cannot be powered on without these resources, a recommendation to power on sufficient standby hosts is made. For more information, see Managing Power Resources.

Related Links

Managing Power Resources on page 3043

The vSphere Distributed Power Management (DPM) feature allows a DRS cluster to reduce its power consumption by powering hosts on and off based on cluster resource utilization.

CPU Virtualization Basics

CPU virtualization emphasizes performance and runs directly on the processor whenever possible. The underlying physical resources are used whenever possible and the virtualization layer runs instructions only as needed to make virtual machines operate as if they were running directly on a physical machine.

CPU virtualization is not the same thing as emulation. ESXi does not use emulation to run virtual CPUs. With emulation, all operations are run in software by an emulator. A software emulator allows programs to run on a computer system other than the one for which they were originally written. The emulator does this by emulating, or reproducing, the original computer's behavior by accepting the same data or inputs and achieving the same results. Emulation provides portability and runs software designed for one platform across several platforms.

When CPU resources are overcommitted, the ESXi host time-slices the physical processors across all virtual machines so each virtual machine runs as if it has its specified number of virtual processors. When an ESXi host runs multiple virtual machines, it allocates to each virtual machine a share of the physical resources. With the default resource allocation settings, all virtual machines associated with the same host receive an equal share of CPU per virtual CPU. This means that a single-processor virtual machines is assigned only half of the resources of a dual-processor virtual machine.

Software-Based CPU Virtualization

With software-based CPU virtualization, the guest application code runs directly on the processor, while the guest privileged code is translated and the translated code runs on the processor.

The translated code is slightly larger and usually runs more slowly than the native version. As a result, guest applications, which have a small privileged code component, run with speeds very close to native. Applications with a significant privileged code component, such as system calls, traps, or page table updates can run slower in the virtualized environment.

Hardware-Assisted CPU Virtualization

Certain processors provide hardware assistance for CPU virtualization.

When using this assistance, the guest can use a separate mode of execution called guest mode. The guest code, whether application code or privileged code, runs in the guest mode. On certain events, the processor exits out of guest mode and enters root mode. The hypervisor executes in the root mode, determines the reason for the exit, takes any required actions, and restarts the guest in guest mode.

When you use hardware assistance for virtualization, there is no need to translate the code. As a result, system calls or trap-intensive workloads run very close to native speed. Some workloads, such as those involving updates to page tables, lead to a large number of exits from guest mode to root mode. Depending on the number of such exits and total time spent in exits, hardware-assisted CPU virtualization can speed up execution significantly.

Virtualization and Processor-Specific Behavior

Although VMware software virtualizes the CPU, the virtual machine detects the specific model of the processor on which it is running.

Processor models might differ in the CPU features they offer, and applications running in the virtual machine can make use of these features. Therefore, it is not possible to use vMotion® to migrate virtual machines between systems running on processors with different feature sets. You can avoid this restriction, in some cases, by using Enhanced vMotion Compatibility (EVC) with processors that support this feature. See the *vCenter Server and Host Management* documentation for more information.

Performance Implications of CPU Virtualization

CPU virtualization adds varying amounts of overhead depending on the workload and the type of virtualization used.

An application is CPU-bound if it spends most of its time executing instructions rather than waiting for external events such as user interaction, device input, or data retrieval. For such applications, the CPU virtualization overhead includes the additional instructions that must be executed. This overhead takes CPU processing time that the application itself can use. CPU virtualization overhead usually translates into a reduction in overall performance.

For applications that are not CPU-bound, CPU virtualization likely translates into an increase in CPU use. If spare CPU capacity is available to absorb the overhead, it can still deliver comparable performance in terms of overall throughput.

ESXi supports up to 128 virtual processors (CPUs) for each virtual machine.

Note: Deploy single-threaded applications on uniprocessor virtual machines, instead of on SMP virtual machines that have multiple CPUs, for the best performance and resource use.

Single-threaded applications can take advantage only of a single CPU. Deploying such applications in dual-processor virtual machines does not speed up the application. Instead, it causes the second virtual CPU to use physical resources that other virtual machines could otherwise use.

Administering CPU Resources

You can configure virtual machines with one or more virtual processors, each with its own set of registers and control structures.

When a virtual machine is scheduled, its virtual processors are scheduled to run on physical processors. The VMkernel Resource Manager schedules the virtual CPUs on physical CPUs, thereby managing the virtual machine's access to physical CPU resources. ESXi supports virtual machines with up to 128 virtual CPUs.

Note: In this chapter, "Memory" can refer to physical RAM or Persistent Memory.

View Processor Information

You can access information about current CPU configuration in the vSphere Client.

1. Browse to the host in the vSphere Client.
2. Under **Hardware**, expand **CPU** to view the information about the number and type of physical processors and the number of logical processors.

   Note: In hyperthreaded systems, each hardware thread is a logical processor. For example, a dual-core processor with hyperthreading activated has two cores and four logical processors.

Specifying CPU Configuration

You can specify CPU configuration to improve resource management. However, if you do not customize CPU configuration, the ESXi host uses defaults that work well in most situations.

You can specify CPU configuration in the following ways:

- Use the attributes and special features available through the vSphere Client. The vSphere Client allows you to connect to the ESXi host or a vCenter Server system.
- Use advanced settings under certain circumstances.
- Use the vSphere SDK for scripted CPU allocation.
- Use hyperthreading.

Related Links

Hyperthreading with vSphere on page 2983

Hyperthreading technology allows a single physical processor core to behave like two logical processors. The processor can run two independent applications at the same time. To avoid confusion between logical and physical processors, Intel refers to a physical processor as a socket, and the discussion in this chapter uses that terminology as well.

Multicore Processors

Multicore processors provide many advantages for a host performing multitasking of virtual machines.

Note: In this topic, "Memory" can refer to physical RAM or Persistent Memory.

Intel and AMD have developed processors which combine two or more processor cores into a single integrated circuit (often called a package or socket). VMware uses the term socket to describe a single package which can have one or more processor cores with one or more logical processors in each core.

A dual-core processor, for example, provides almost double the performance of a single-core processor, by allowing two virtual CPUs to run at the same time. Cores within the same processor are typically configured with a shared last-

level cache used by all cores, potentially reducing the need to access slower main memory. A shared memory bus that connects a physical processor to main memory can limit performance of its logical processors when the virtual machines running on them are running memory-intensive workloads which compete for the same memory bus resources.

Each logical processor of each processor core is used independently by the ESXi CPU scheduler to run virtual machines, providing capabilities similar to SMP systems. For example, a two-way virtual machine can have its virtual processors running on logical processors that belong to the same core, or on logical processors on different physical cores.

The ESXi CPU scheduler can detect the processor topology and the relationships between processor cores and the logical processors on them. It uses this information to schedule virtual machines and optimize performance.

The ESXi CPU scheduler can interpret processor topology, including the relationship between sockets, cores, and logical processors. The scheduler uses topology information to optimize the placement of virtual CPUs onto different sockets. This optimization can maximize overall cache usage, and to improve cache affinity by minimizing virtual CPU migrations.

Hyperthreading with vSphere

Hyperthreading technology allows a single physical processor core to behave like two logical processors. The processor can run two independent applications at the same time. To avoid confusion between logical and physical processors, Intel refers to a physical processor as a socket, and the discussion in this chapter uses that terminology as well.

Intel Corporation developed hyperthreading technology to enhance the performance of its Pentium IV and Xeon processor lines. Hyperthreading technology allows a single processor core to execute two independent threads simultaneously.

While hyperthreading does not double the performance of a system, it can increase performance by better utilizing idle resources leading to greater throughput for certain important workload types. An application running on one logical processor of a busy core can expect slightly more than half of the throughput that it obtains while running alone on a non-hyperthreaded processor. Hyperthreading performance improvements are highly application-dependent, and some applications might see performance degradation with hyperthreading because many processor resources (such as the cache) are shared between logical processors.

Note: On processors with Intel Hyper-Threading technology, each core can have two logical processors which share most of the core's resources, such as memory caches and functional units. Such logical processors are usually called threads.

Some processors do not support hyperthreading and as a result have only one thread per core. For such processors, the number of cores also matches the number of logical processors.

Hyperthreading and ESXi Hosts

A host that is enabled for hyperthreading should behave similarly to a host without hyperthreading. You might need to consider certain factors if you enable hyperthreading, however.

ESXi hosts manage processor time intelligently to guarantee that load is spread smoothly across processor cores in the system. Logical processors on the same core have consecutive CPU numbers, so that CPUs 0 and 1 are on the first core together, CPUs 2 and 3 are on the second core, and so on. Virtual machines are preferentially scheduled on two different cores rather than on two logical processors on the same core.

If there is no work for a logical processor, it is put into a halted state, which frees its execution resources and allows the virtual machine running on the other logical processor on the same core to use the full execution resources of the core. The VMware scheduler properly accounts for this halt time, and charges a virtual machine running with the full resources of a core more than a virtual machine running on a half core. This approach to processor management ensures that the server does not violate any of the standard ESXi resource allocation rules.

Consider your resource management needs before you enable CPU affinity on hosts using hyperthreading. For example, if you bind a high priority virtual machine to CPU 0 and another high priority virtual machine to CPU 1, the two virtual machines have to share the same physical core. In this case, it can be impossible to meet the resource demands of these virtual machines. Ensure that any custom affinity settings make sense for a hyperthreaded system.

Enable Hyperthreading

To enable hyperthreading, you must first enable it in your system's BIOS settings and then turn it on in the vSphere Client. Hyperthreading is enabled by default.

Consult your system documentation to determine whether your CPU supports hyperthreading.

1. Ensure that your system supports hyperthreading technology.
2. Enable hyperthreading in the system BIOS.
   Some manufacturers label this option **Logical Processor**, while others call it **Enable Hyperthreading**.
3. Ensure that hyperthreading is enabled for the ESXi host.
   a) Browse to the host in the vSphere Client.
   b) Click **Configure**.
   c) Under **System**, click **Advanced System Settings** and select **VMkernel.Boot.hyperthreading**.
   You must restart the host for the setting to take effect. Hyperthreading is enabled if the value is `true`.
4. Under **Hardware**, click **Processors** to view the number of Logical processors.

Hyperthreading is enabled.

Using CPU Affinity

By specifying a CPU affinity setting for each virtual machine, you can restrict the assignment of virtual machines to a subset of the available processors in multiprocessor systems. By using this feature, you can assign each virtual machine to processors in the specified affinity set.

CPU affinity specifies virtual machine-to-processor placement constraints and is different from the relationship created by a VM-VM or VM-Host affinity rule, which specifies virtual machine-to-virtual machine host placement constraints.

In this context, the term CPU refers to a logical processor on a hyperthreaded system and refers to a core on a non-hyperthreaded system.

The CPU affinity setting for a virtual machine applies to all of the virtual CPUs associated with the virtual machine and to all other threads (also known as worlds) associated with the virtual machine. Such virtual machine threads perform processing required for emulating mouse, keyboard, screen, CD-ROM, and miscellaneous legacy devices.

In some cases, such as display-intensive workloads, significant communication might occur between the virtual CPUs and these other virtual machine threads. Performance might degrade if the virtual machine's affinity setting prevents these additional threads from being scheduled concurrently with the virtual machine's virtual CPUs. Examples of this include a uniprocessor virtual machine with affinity to a single CPU or a two-way SMP virtual machine with affinity to only two CPUs.

For the best performance, when you use manual affinity settings, VMware recommends that you include at least one additional physical CPU in the affinity setting to allow at least one of the virtual machine's threads to be scheduled at the same time as its virtual CPUs. Examples of this include a uniprocessor virtual machine with affinity to at least two CPUs or a two-way SMP virtual machine with affinity to at least three CPUs.

Assign a Virtual Machine to a Specific Processor

Using CPU affinity, you can assign a virtual machine to a specific processor. This allows you to restrict the assignment of virtual machines to a specific available processor in multiprocessor systems.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Select **VMs**.
2. Right-click the virtual machine and click **Edit Settings**.
3. Under Virtual Hardware, expand **CPU**.
4. Under Scheduling Affinity, select physical processor affinity for the virtual machine.
   Use '-' for ranges and ',' to separate values.
   For example, "0, 2, 4-7" would indicate processors 0, 2, 4, 5, 6 and 7.
5. Select the processors where you want the virtual machine to run and click **OK**.

Potential Issues with CPU Affinity

Before you use CPU affinity, you might need to consider certain issues.

Potential issues with CPU affinity include:

- For multiprocessor systems, ESXi systems perform automatic load balancing. Avoid manual specification of virtual machine affinity to improve the scheduler's ability to balance load across processors.
- Affinity can interfere with the ESXi host's ability to meet the reservation and shares specified for a virtual machine.
- Because CPU admission control does not consider affinity, a virtual machine with manual affinity settings might not always receive its full reservation.
  Virtual machines that do not have manual affinity settings are not adversely affected by virtual machines with manual affinity settings.
- When you move a virtual machine from one host to another, affinity might no longer apply because the new host might have a different number of processors.
- The NUMA scheduler might not be able to manage a virtual machine that is already assigned to certain processors using affinity. For more information, see Using NUMA Systems with ESXi.
- Affinity can affect the host's ability to schedule virtual machines on multicore or hyperthreaded processors to take full advantage of resources shared on such processors.

Related Links

Using NUMA Systems with ESXi on page 3063

ESXi supports memory access optimization for Intel and AMD Opteron processors in server architectures that support NUMA (non-uniform memory access).

Host Power Management Policies

You can apply several power management features in ESXi that the host hardware provides to adjust the balance between performance and power. You can control how ESXi uses these features by selecting a power management policy.

Selecting a high-performance policy provides more absolute performance, but at lower efficiency and performance per watt. Low-power policies provide less absolute performance, but at higher efficiency.

You can select a policy for the host that you manage by using the VMware Host Client. If you do not select a policy, ESXi uses Balanced by default.

Table 330: CPU Power Management Policies

Power Management Policy	Description
High Performance	Do not use any power management features.
Balanced (Default)	Reduce energy consumption with minimal performance compromise
Low Power	Reduce energy consumption at the risk of lower performance
Custom	User-defined power management policy. Advanced configuration becomes available.

When a CPU runs at lower frequency, it can also run at lower voltage, which saves power. This type of power management is typically called Dynamic Voltage and Frequency Scaling (DVFS). ESXi attempts to adjust CPU frequencies so that virtual machine performance is not affected.

When a CPU is idle, ESXi can apply deep halt states, also known as C-states. The deeper the C-state, the less power the CPU uses, but it also takes longer for the CPU to start running again. When a CPU becomes idle, ESXi applies an algorithm to predict the idle state duration and chooses an appropriate C-state to enter. In power management policies that do not use deep C-states, ESXi uses only the shallowest halt state for idle CPUs, C1.

Select a CPU Power Management Policy

You set the CPU power management policy for a host using the vSphere Client.

Verify that the BIOS settings on the host system allow the operating system to control power management (for example, **OS Controlled**). If the host hardware does not allow the operating system to manage power, only the Not Supported policy is available. (On some systems, only the High Performance policy is available.)

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under Hardware, select Overview and click **Edit Power Policy**.
4. Select a power management policy for the host and click **OK**.

   The policy selection is saved in the host configuration and can be used again at boot time. You can change it at any time, and it does not require a server reboot.

Configure Custom Policy Parameters for Host Power Management

When you use the Custom policy for host power management, ESXi bases its power management policy on the values of several advanced configuration parameters.

Select **Custom** for the power management policy, as described in Select a CPU Power Management Policy.

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under **System**, select **Advanced System Settings**.
4. In the right pane, you can edit the power management parameters that affect the Custom policy.

   Power management parameters that affect the Custom policy have descriptions that begin with **In Custom policy**. All other power parameters affect all power management policies.

5. Select the parameter and click the **Edit** button.

   Note: The default values of power management parameters match the Balanced policy.

Parameter	Description
Power.UsePStates	Use ACPI P-states to save power when the processor is busy.
Power.MaxCpuLoad	Use P-states to save power on a CPU only when the CPU is busy for less than the given percentage of real time.
Power.MinFreqPct	Do not use any P-states slower than the given percentage of full CPU speed.
Power.UseStallCtr	Use a deeper P-state when the processor is frequently stalled waiting for events such as cache misses.
Power.TimerHz	Controls how many times per second ESXi reevaluates which P-state each CPU should be in.
Power.UseCStates	Use deep ACPI C-states (C2 or below) when the processor is idle.
Power.CStateMaxLatency	Do not use C-states whose latency is greater than this value.
Power.CStateResidencyCoef	When a CPU becomes idle, choose the deepest C-state whose latency multiplied by this value is less than the host's prediction of how long the CPU will remain idle. Larger values make ESXi more conservative about using deep C-states, while smaller values are more aggressive.
Power.CStatePredictionCoef	A parameter in the ESXi algorithm for predicting how long a CPU that becomes idle will remain idle. Changing this value is not recommended.
Power.PerfBias	Performance Energy Bias Hint (Intel-only). Sets an MSR on Intel processors to an Intel-recommended value. Intel recommends 0 for high performance, 6 for balanced, and 15 for low power. Other values are undefined.

6. Click **OK**.

Memory Virtualization Basics

Before you manage memory resources, you should understand how they are being virtualized and used by ESXi.

The VMkernel manages all physical RAM on the host. The VMkernel dedicates part of this managed physical RAM for its own use. The rest is available for use by virtual machines.

The virtual and physical memory space is divided into blocks called pages. When physical memory is full, the data for virtual pages that are not present in physical memory are stored on disk. Depending on processor architecture, pages are typically 4 KB or 2 MB. See Advanced Memory Attributes.

Virtual Machine Memory

Each virtual machine consumes memory based on its configured size, plus additional overhead memory for virtualization.

The configured size is the amount of memory that is presented to the guest operating system. This is different from the amount of physical RAM that is allocated to the virtual machine. The latter depends on the resource settings (shares, reservation, limit) and the level of memory pressure on the host.

For example, consider a virtual machine with a configured size of 1GB. When the guest operating system boots, it detects that it is running on a dedicated machine with 1GB of physical memory. In some cases, the virtual machine might be allocated the full 1GB. In other cases, it might receive a smaller allocation. Regardless of the actual allocation, the guest operating system continues to behave as though it is running on a dedicated machine with 1GB of physical memory.

Shares	Specify the relative priority for a virtual machine if more than the reservation is available.
Reservation	Is a guaranteed lower bound on the amount of physical RAM that the host reserves for the virtual machine, even when memory is overcommitted. Set the reservation to a level that ensures the virtual machine has sufficient memory to run efficiently, without excessive paging. After a virtual machine consumes all of the memory within its reservation, it is allowed to retain that amount of memory and this memory is not reclaimed, even if the virtual machine becomes idle. Some guest operating systems (for example, Linux) might not access all of the configured memory immediately after booting. Until the virtual machines consumes all of the memory within its reservation, VMkernel can allocate any unused portion of its reservation to other virtual machines. However, after the guest's workload increases and the virtual machine consumes its full reservation, it is allowed to keep this memory.
Limit	Is an upper bound on the amount of physical RAM that the host can allocate to the virtual machine. The virtual machine's memory allocation is also implicitly limited by its configured size.

Memory Overcommitment

For each running virtual machine, the system reserves physical RAM for the virtual machine's reservation (if any) and for its virtualization overhead.

The total configured memory sizes of all virtual machines may exceed the amount of available physical memory on the host. However, it doesn't necessarily mean memory is overcommitted. Memory is overcommitted when the combined working memory footprint of all virtual machines exceed that of the host memory sizes.

Because of the memory management techniques the ESXi host uses, your virtual machines can use more virtual RAM than there is physical RAM available on the host. For example, you can have a host with 2GB memory and run four virtual machines with 1GB memory each. In that case, the memory is overcommitted. For instance, if all four virtual machines are idle, the combined consumed memory may be well below 2GB. However, if all 4GB virtual machines are actively consuming memory, then their memory footprint may exceed 2GB and the ESXi host will become overcommitted.

Overcommitment makes sense because, typically, some virtual machines are lightly loaded while others are more heavily loaded, and relative activity levels vary over time.

To improve memory utilization, the ESXi host transfers memory from idle virtual machines to virtual machines that need more memory. Use the Reservation or Shares parameter to preferentially allocate memory to important virtual machines. This memory remains available to other virtual machines if it is not in use. ESXi implements various mechanisms such as ballooning, memory sharing, memory compression and swapping to provide reasonable performance even if the host is not heavily memory overcommitted.

An ESXi host can run out of memory if virtual machines consume all reservable memory in a memory overcommitted environment. Although the powered on virtual machines are not affected, a new virtual machine might fail to power on due to lack of memory.

Note: All virtual machine memory overhead is also considered reserved.

In addition, memory compression is enabled by default on ESXi hosts to improve virtual machine performance when memory is overcommitted as described in Memory Compression.

Memory Sharing

Memory sharing is a proprietary ESXi technique that can help achieve greater memory density on a host.

Memory sharing relies on the observation that several virtual machines might be running instances of the same guest operating system. These virtual machines might have the same applications or components loaded, or contain common data. In such cases, a host uses a proprietary Transparent Page Sharing (TPS) technique to eliminate redundant copies of memory pages. With memory sharing, a workload running on a virtual machine often consumes less memory than it might when running on physical machines. As a result, higher levels of overcommitment can be supported efficiently. The amount of memory saved by memory sharing depends on whether the workload consists of nearly identical machines which might free up more memory. A more diverse workload might result in a lower percentage of memory savings.

Note:

Due to security concerns, inter-virtual machine transparent page sharing is deactivated by default and page sharing is being restricted to intra-virtual machine memory sharing. Page sharing does not occur across virtual machines and only occurs inside a virtual machine. See Sharing Memory Across Virtual Machines for more information.

Memory Virtualization

Because of the extra level of memory mapping introduced by virtualization, ESXi can effectively manage memory across all virtual machines.

Some of the physical memory of a virtual machine might be mapped to shared pages or to pages that are unmapped, or swapped out.

A host performs virtual memory management without the knowledge of the guest operating system and without interfering with the guest operating system's own memory management subsystem.

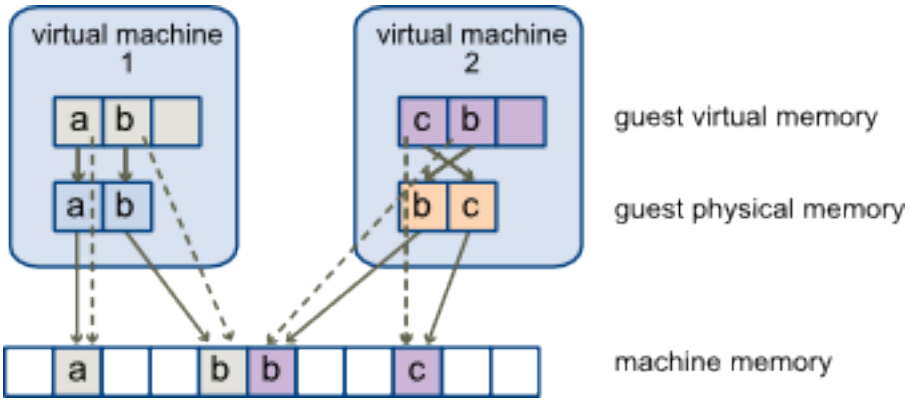
The VMM for each virtual machine maintains a mapping from the guest operating system's physical memory pages to the physical memory pages on the underlying machine. (VMware refers to the underlying host physical pages as "machine" pages and the guest operating system's physical pages as "physical" pages.)

Each virtual machine sees a contiguous, zero-based, addressable physical memory space. The underlying machine memory on the server used by each virtual machine is not necessarily contiguous.

The guest virtual to guest physical addresses are managed by the guest operating system. The hypervisor is only responsible for translating the guest physical addresses to machine addresses. Hardware-assisted memory virtualization utilizes the hardware facility to generate the combined mappings with the guest's page tables and the nested page tables maintained by the hypervisor.

The diagram illustrates the ESXi implementation of memory virtualization.

Figure 97: ESXi Memory Mapping



- The boxes represent pages, and the arrows show the different memory mappings.

- The arrows from guest virtual memory to guest physical memory show the mapping maintained by the page tables in the guest operating system. (The mapping from virtual memory to linear memory for x86-architecture processors is not shown.)
- The arrows from guest physical memory to machine memory show the mapping maintained by the VMM.
- The dashed arrows show the mapping from guest virtual memory to machine memory in the shadow page tables also maintained by the VMM. The underlying processor running the virtual machine uses the shadow page table mappings.

Hardware-Assisted Memory Virtualization

Some CPUs, such as AMD SVM-V and the Intel Xeon 5500 series, provide hardware support for memory virtualization by using two layers of page tables.

Note: In this topic, "Memory" can refer to physical RAM or Persistent Memory.

The first layer of page tables stores guest virtual-to-physical translations, while the second layer of page tables stores guest physical-to-machine translation. The TLB (translation look-aside buffer) is a cache of translations maintained by the processor's memory management unit (MMU) hardware. A TLB miss is a miss in this cache and the hardware needs to go to memory (possibly many times) to find the required translation. For a TLB miss to a certain guest virtual address, the hardware looks at both page tables to translate guest virtual address to machine address. The first layer of page tables is maintained by the guest operating system. The VMM only maintains the second layer of page tables.

Performance Considerations

When you use hardware assistance, you eliminate the overhead for software memory virtualization. In particular, hardware assistance eliminates the overhead required to keep shadow page tables in synchronization with guest page tables. However, the TLB miss latency when using hardware assistance is significantly higher. By default the hypervisor uses large pages in hardware assisted modes to reduce the cost of TLB misses. As a result, whether or not a workload benefits by using hardware assistance primarily depends on the overhead the memory virtualization causes when using software memory virtualization. If a workload involves a small amount of page table activity (such as process creation, mapping the memory, or context switches), software virtualization does not cause significant overhead. Conversely, workloads with a large amount of page table activity are likely to benefit from hardware assistance.

By default the hypervisor uses large pages in hardware assisted modes to reduce the cost of TLB misses. The best performance is achieved by using large pages in both guest virtual to guest physical and guest physical to machine address translations.

The option `LPage.LPageAlwaysTryForNPT` can change the policy for using large pages in guest physical to machine address translations. For more information, see Advanced Memory Attributes.

Support for Large Page Sizes

ESXi provides limited support for large page sizes.

x86 architecture allows system software to use 4KB, 2MB and 1GB pages. We refer to 4KB pages as small pages while 2MB and 1GB pages are referred to as large pages. Large pages relieve translation lookaside buffer (TLB) pressure and reduce the cost of page table walks, which results in improved workload performance.

In virtualized environments, large pages can be used by the hypervisor and the guest operating system independently. While the biggest performance impact is achieved if large pages are used by the guest and the hypervisor, in most cases a performance impact can be observed even if large pages are used only at the hypervisor level.

ESXi hypervisor uses 2MB pages for backing guest vRAM by default. vSphere 6.7 ESXi provides a limited support for backing guest vRAM with 1GB pages. For more information, see *Backing Guest vRAM with 1GB Pages*.

Administering Memory Resources

Using the vSphere Client you can view information about and make changes to memory allocation settings. To administer your memory resources effectively, you must also be familiar with memory overhead, idle memory tax, and how ESXi hosts reclaim memory.

When administering memory resources, you can specify memory allocation. If you do not customize memory allocation, the ESXi host uses defaults that work well in most situations.

You can specify memory allocation in several ways.

- Use the attributes and special features available through the vSphere Client. The vSphere Client allows you to connect to the ESXi host or vCenter Server system.
- Use advanced settings.
- Use the vSphere SDK for scripted memory allocation.

Note: In this chapter, "Memory" can refer to physical RAM or Persistent Memory.

Understanding Memory Overhead

Virtualization of memory resources has some associated overhead.

ESXi virtual machines can incur two kinds of memory overhead.

- The additional time to access memory within a virtual machine.
- The extra space needed by the ESXi host for its own code and data structures, beyond the memory allocated to each virtual machine.

ESXi memory virtualization adds little time overhead to memory accesses. Because the processor's paging hardware uses page tables (shadow page tables for software-based approach or two level page tables for hardware-assisted approach) directly, most memory accesses in the virtual machine can execute without address translation overhead.

The memory space overhead has two components.

- A fixed, system-wide overhead for the VMkernel.
- Additional overhead for each virtual machine.

Overhead memory includes space reserved for the virtual machine frame buffer and various virtualization data structures, such as shadow page tables. Overhead memory depends on the number of virtual CPUs and the configured memory for the guest operating system.

Overhead Memory on Virtual Machines

Virtual machines require a certain amount of available overhead memory to power on. You should be aware of the amount of this overhead.

The amount of overhead memory needed for a virtual machine depends on a large number of factors, including the number of vCPUs and memory size, the number and types of devices, the execution mode that the monitor is using and the hardware version of the virtual machine. The version of vSphere you are using can also effect the amount of memory needed. VMX automatically calculates the amount of overhead memory needed for a virtual machine.

In order to find out how much overhead memory is needed for your specific configuration, first power on the virtual machine in question. Look in the vmware.log file. When the virtual machine powers on, the amount of overhead memory it needs is printed to the log. Search within the log for `VMMEM` to see the initial and precise amount of overhead memory reserved for the virtual machine.

How ESXi Hosts Allocate Memory

A host allocates the memory specified by the `Limit` parameter to each virtual machine, unless memory is overcommitted. ESXi never allocates more memory to a virtual machine than its specified physical memory size.

For example, a 1GB virtual machine might have the default limit (unlimited) or a user-specified limit (for example 2GB). In both cases, the ESXi host never allocates more than 1GB, the physical memory size that was specified for it.

When memory is overcommitted, each virtual machine is allocated an amount of memory somewhere between what is specified by **Reservation** and what is specified by **Limit**. The amount of memory granted to a virtual machine above its reservation usually varies with the current memory load.

A host determines allocations for each virtual machine based on the number of shares allocated to it and an estimate of its recent working set size.

- Shares — ESXi hosts use a modified proportional-share memory allocation policy. Memory shares entitle a virtual machine to a fraction of available physical memory.
- Working set size — ESXi hosts estimate the working set for a virtual machine by monitoring memory activity over successive periods of virtual machine execution time. Estimates are smoothed over several time periods using techniques that respond rapidly to increases in working set size and more slowly to decreases in working set size.
  This approach ensures that a virtual machine from which idle memory is reclaimed can ramp up quickly to its full share-based allocation when it starts using its memory more actively.
  Memory activity is monitored to estimate the working set sizes for a default period of 60 seconds. To modify this default , adjust the `Mem.SamplePeriod` advanced setting. See Set Advanced Host Attributes.

Memory Tax for Idle Virtual Machines

If a virtual machine is not actively using all of its currently allocated memory, ESXi charges more for idle memory than for memory that is in use. This is done to help prevent virtual machines from hoarding idle memory.

The idle memory tax is applied in a progressive fashion. The effective tax rate increases as the ratio of idle memory to active memory for the virtual machine rises. (In earlier versions of ESXi that did not support hierarchical resource pools, all idle memory for a virtual machine was taxed equally.)

You can modify the idle memory tax rate with the `Mem.IdleTax` option. Use this option, together with the `Mem.SamplePeriod` advanced attribute, to control how the system determines target memory allocations for virtual machines. See Set Advanced Host Attributes.

Note: In most cases, changes to `Mem.IdleTax` are not necessary nor appropriate.

VMX Swap Files

Virtual machine executable (VMX) swap files allow the host to greatly reduce the amount of overhead memory reserved for the VMX process.

Note: VMX swap files are not related to the swap to host swap cache feature or to regular host-level swap files.

ESXi reserves memory per virtual machine for a variety of purposes. Memory for the needs of certain components, such as the virtual machine monitor (VMM) and virtual devices, is fully reserved when a virtual machine is powered on. However, some of the overhead memory that is reserved for the VMX process can be swapped. The VMX swap feature reduces the VMX memory reservation significantly (for example, from about 50MB or more per virtual machine to about 10MB per virtual machine). This allows the remaining memory to be swapped out when host memory is overcommitted, reducing overhead memory reservation for each virtual machine.

The host creates VMX swap files automatically, provided there is sufficient free disk space at the time a virtual machine is powered on.

Memory Reclamation

ESXi hosts can reclaim memory from virtual machines.

A host allocates the amount of memory specified by a reservation directly to a virtual machine. Anything beyond the reservation is allocated using the host's physical resources or, when physical resources are not available, handled using special techniques such as ballooning or swapping. Hosts can use two techniques for dynamically expanding or contracting the amount of memory allocated to virtual machines.

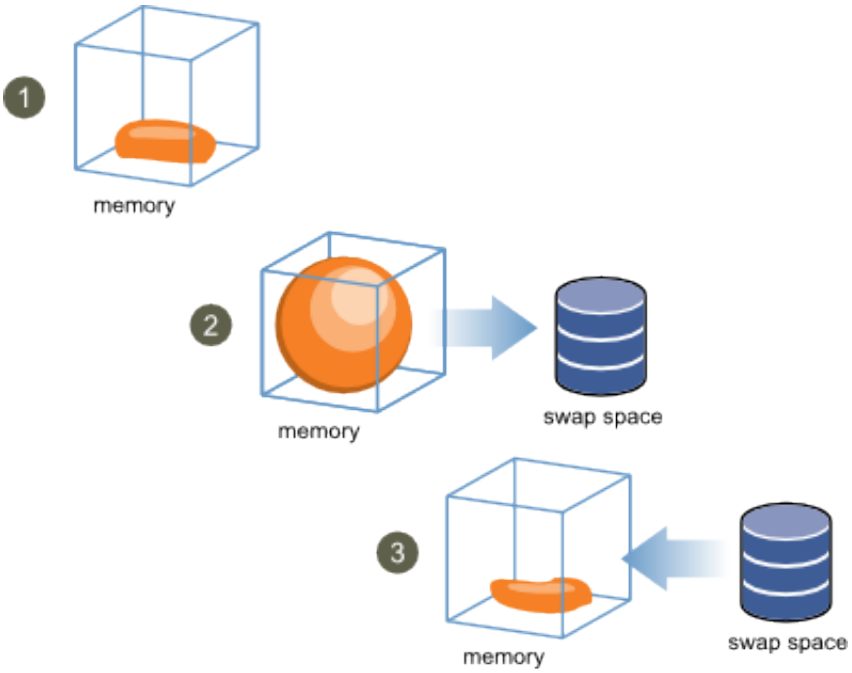
- ESXi systems use a memory balloon driver (`vmmemctl`), loaded into the guest operating system running in a virtual machine. See Memory Balloon Driver.
- ESXi system swaps out a page from a virtual machine to a server swap file without any involvement by the guest operating system. Each virtual machine has its own swap file.

Memory Balloon Driver

The memory balloon driver (`vmmemctl`) collaborates with the server to reclaim pages that are considered least valuable by the guest operating system.

The driver uses a proprietary ballooning technique that provides predictable performance that closely matches the behavior of a native system under similar memory constraints. This technique increases or decreases memory pressure on the guest operating system, causing the guest to use its own native memory management algorithms. When memory is tight, the guest operating system determines which pages to reclaim and, if necessary, swaps them to its own virtual disk.

Figure 98: Memory Ballooning in the Guest Operating System



Note: You must configure the guest operating system with sufficient swap space. Some guest operating systems have additional limitations.

If necessary, you can limit the amount of memory `vmmemctl` reclaims by setting the **sched.mem.maxmemctl** parameter for a specific virtual machine. This option specifies the maximum amount of memory that can be reclaimed from a virtual machine in megabytes (MB). See Set Advanced Virtual Machine Attributes.

Using Swap Files

You can specify the location of your guest swap file, reserve swap space when memory is overcommitted, and delete a swap file.

ESXi hosts use swapping to forcibly reclaim memory from a virtual machine when the `vmmemctl` driver is not available or is not responsive.

- It was never installed.
- It is explicitly deactivated.
- It is not running (for example, while the guest operating system is booting).
- It is temporarily unable to reclaim memory quickly enough to satisfy current system demands.
- It is functioning properly, but maximum balloon size is reached.

Standard demand-paging techniques swap pages back in when the virtual machine needs them.

Swap File Location

By default, the swap file is created in the same location as the virtual machine's configuration file, which may either be on a VMFS datastore, a vSAN datastore or a VMware vSphere® Virtual VolumesTM datastore. On a vSAN datastore or a vVols datastore, the swap file is created as a separate vSAN or vVols object.

The ESXi host creates a swap file when a virtual machine is powered on. If this file cannot be created, the virtual machine cannot power on. Instead of accepting the default, you can also:

- Use per-virtual machine configuration options to change the datastore to another shared storage location.
- Use host-local swap, which allows you to specify a datastore stored locally on the host. This allows you to swap at a per-host level, saving space on the SAN. However, it can lead to a slight degradation in performance for vSphere vMotion because pages swapped to a local swap file on the source host must be transferred across the network to the destination host. Currently vSAN and vVols datastores cannot be specified for host-local swap.

Enable Host-Local Swap for a DRS Cluster

Host-local swap allows you to specify a datastore stored locally on the host as the swap file location. You can enable host-local swap for a DRS cluster.

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Configuration**, select **General** to view the swap file location and click **Edit** to change it.
4. Select the **Datastore specified by host** option and click **OK**.
5. Browse to one of the hosts in the cluster in the vSphere Client.
6. Click **Configure**.
7. Under Virtual Machines, select **Swap file location**.
8. Click Edit and select the local datastore to use and click **OK**.
9. Repeat 5 through 8 for each host in the cluster.

Host-local swap is now enabled for the DRS cluster.

Enable Host-Local Swap for a Standalone Host

Host-local swap allows you to specify a datastore stored locally on the host as the swap file location. You can enable host-local swap for a standalone host.

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under **Virtual Machines**, select **Swap file location**.
4. Click **Edit** and select **Selected Datastore**.
5. Select a local datastore from the list and click **OK**.

Host-local swap is now enabled for the standalone host.

Swap Space and Memory Overcommitment

You must reserve swap space for any unreserved virtual machine memory (the difference between the reservation and the configured memory size) on per-virtual machine swap files.

This swap reservation is required to ensure that the ESXi host is able to preserve virtual machine memory under any circumstances. In practice, only a small fraction of the host-level swap space might be used.

If you are overcommitting memory with ESXi, to support the intra-guest swapping induced by ballooning, ensure that your guest operating systems also have sufficient swap space. This guest-level swap space must be greater than or equal to the difference between the virtual machine's configured memory size and its Reservation.

CAUTION: If memory is overcommitted, and the guest operating system is configured with insufficient swap space, the guest operating system in the virtual machine can fail.

To prevent virtual machine failure, increase the size of the swap space in your virtual machines.

- Windows guest operating systems— Windows operating systems refer to their swap space as paging files. Some Windows operating systems try to increase the size of paging files automatically, if there is sufficient free disk space. See your Microsoft Windows documentation or search the Windows help files for "paging files." Follow the instructions for changing the size of the virtual memory paging file.
- Linux guest operating system — Linux operating systems refer to their swap space as swap files. For information on increasing swap files, see the following Linux man pages:
  - `mkswap` — Sets up a Linux swap area.
  - `swapon` — Enables devices and files for paging and swapping.

Guest operating systems with a lot of memory and small virtual disks (for example, a virtual machine with 8GB RAM and a 2GB virtual disk) are more susceptible to having insufficient swap space.

Note: Do not store swap files on thin-provisioned LUNs. Running a virtual machine with a swap file that is stored on a thin-provisioned LUN can cause swap file growth failure, which can lead to termination of the virtual machine.

When you create a large swap file (for example, larger than 100GB), the amount of time it takes for the virtual machine to power on can increase significantly. To avoid this, set a high reservation for large virtual machines.

You can also place swap files on less costly storage using host-local swap files.

Configure Virtual Machine Swapfile Properties for the Host

Configure a swapfile location for the host to determine the default location for virtual machine swapfiles in the vSphere Client.

Required privilege:**Host machine** > **Configuration** > **Storage partition configuration**

By default, swapfiles for a virtual machine are located on a datastore in the folder that contains the other virtual machine files. However, you can configure your host to place virtual machine swapfiles on an alternative datastore.

You can use this option to place virtual machine swapfiles on lower-cost or higher-performance storage. You can also override this host-level setting for individual virtual machines.

Setting an alternative swapfile location might cause migrations with vMotion to complete more slowly. For best vMotion performance, store the virtual machine on a local datastore rather than in the same directory as the virtual machine swapfiles. If the virtual machine is stored on a local datastore, storing the swapfile with the other virtual machine files will not improve vMotion.

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under **Virtual Machines**, click **Swap file location**.

   The selected swapfile location is displayed. If configuration of the swapfile location is not supported on the selected host, the tab indicates that the feature is not supported.

   If the host is part of a cluster, and the cluster settings specify that swapfiles are to be stored in the same directory as the virtual machine, you cannot edit the swapfile location from the host under **Configure**. To change the swapfile location for such a host, edit the cluster settings.
4. Click **Edit**.
5. Select where to store the swapfile.

Option	Description
Virtual machine directory	Stores the swapfile in the same directory as the virtual machine configuration file.
Use a specific datastore	Stores the swapfile in the location you specify. If the swapfile cannot be stored on the datastore that the host specifies, the swapfile is stored in the same folder as the virtual machine.

6. Optional: If you select **Use a specific datastore**, select a datastore from the list.
7. Click **OK**.

The virtual machine swapfile is stored in the location you selected.

Configure a Virtual Machine Swap File Location for a Cluster

By default, swap files for a virtual machine are on a datastore in the folder that contains the other virtual machine files. However, you can instead configure the hosts in your cluster to place virtual machine swap files on an alternative datastore of your choice.

Before you configure a virtual machine swap file location for a cluster, you must configure the virtual machine swap file locations for the hosts in the cluster as described in Configure Virtual Machine Swapfile Properties for the Host.

You can configure an alternative swap file location to place virtual machine swap files on either lower-cost or higher-performance storage, depending on your needs.

1. Browse to the cluster.
2. Click **Configure**.
3. Select **Configuration** > **General**.
4. Next to swap file location, click **Edit**.
5. Select where to store the swap file.

Option	Description
Virtual machine directory	Stores the swap file in the same directory as the virtual machine configuration file.
Datastore specified by host	Stores the swap file in the location specified in the host configuration. If the swap file cannot be stored on the datastore that the host specifies, the swap file is stored in the same folder as the virtual machine.

6. Click **OK**.

Delete Swap Files

If a host fails, and that host had running virtual machines that were using swap files, those swap files continue to exist and consume many gigabytes of disk space. You can delete the swap files to eliminate this problem.

1. Restart the virtual machine that was on the host that failed.
2. Stop the virtual machine.

The swap file for the virtual machine is deleted.

Sharing Memory Across Virtual Machines

Many ESXi workloads present opportunities for sharing memory across virtual machines (as well as within a single virtual machine).

ESXi memory sharing runs as a background activity that scans for sharing opportunities over time. The amount of memory saved varies over time. For a fairly constant workload, the amount generally increases slowly until all sharing opportunities are exploited.

To determine the effectiveness of memory sharing for a given workload, try running the workload, and use `resxtop` or `esxtop` to observe the actual savings. Find the information in the `PSHARE` field of the interactive mode in the Memory page.

Use the `Mem.ShareScanTime` and `Mem.ShareScanGHz` advanced settings to control the rate at which the system scans memory to identify opportunities for sharing memory.

You can also configure sharing for individual virtual machines by setting the `sched.mem.pshare.enable` option.

Due to security concerns, inter-virtual machine transparent page sharing is deactivated by default and page sharing is being restricted to intra-virtual machine memory sharing. This means page sharing does not occur across virtual machines and only occurs inside of a virtual machine. The concept of salting has been introduced to help address concerns system administrators may have over the security implications of transparent page sharing. Salting can be used to allow more

granular management of the virtual machines participating in transparent page sharing than was previously possible. With the new salting settings, virtual machines can share pages only if the salt value and contents of the pages are identical. A new host config option `Mem.ShareForceSalting` can be configured to activate or deactivate salting.

See Advanced Attributes for information on how to set advanced options.

Memory Compression

ESXi provides a memory compression cache to improve virtual machine performance when you use memory overcommitment. Memory compression is activated by default. When a host's memory becomes overcommitted, ESXi compresses virtual pages and stores them in memory.

Because accessing compressed memory is faster than accessing memory that is swapped to disk, memory compression in ESXi allows you to overcommit memory without significantly hindering performance. When a virtual page needs to be swapped, ESXi first attempts to compress the page. Pages that can be compressed to 2 KB or smaller are stored in the virtual machine's compression cache, increasing the capacity of the host.

You can set the maximum size for the compression cache and deactivate memory compression using the Advanced Settings dialog box in the vSphere Client.

Activate or Deactivate the Memory Compression Cache

Memory compression is activated by default. You can use Advanced System Settings in the vSphere Client to activate or deactivate memory compression for a host.

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under **System**, select **Advanced System Settings**.
4. Locate Mem.MemZipEnable and click the **Edit** button.
5. Enter 1 to activate or enter 0 to deactivate the memory compression cache.
6. Click **OK**.

Set the Maximum Size of the Memory Compression Cache

You can set the maximum size of the memory compression cache for the host's virtual machines.

You set the size of the compression cache as a percentage of the memory size of the virtual machine. For example, if you enter 20 and a virtual machine's memory size is 1000 MB, ESXi can use up to 200MB of host memory to store the compressed pages of the virtual machine.

If you do not set the size of the compression cache, ESXi uses the default value of 10 percent.

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under **System**, select **Advanced System Settings**.
4. Locate Mem.MemZipMaxPct and click the **Edit** button.
   The value of this attribute determines the maximum size of the compression cache for the virtual machine.
5. Enter the maximum size for the compression cache.
   The value is a percentage of the size of the virtual machine and must be between 5 and 100 percent.

6. Click **OK**.

Measuring and Differentiating Types of Memory Usage

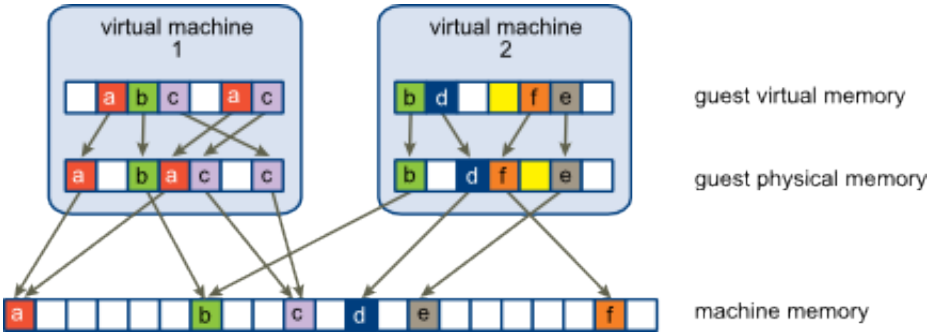
The **Performance** tab of the vSphere Client displays several metrics that can be used to analyze memory usage.

Some of these memory metrics measure guest physical memory while other metrics measure machine memory. For instance, two types of memory usage that you can examine using performance metrics are guest physical memory and machine memory. You measure guest physical memory using the Memory Granted metric (for a virtual machine) or Memory Shared (for a host). To measure machine memory, however, use Memory Consumed (for a virtual machine) or Memory Shared Common (for a host). Understanding the conceptual difference between these types of memory usage is important for knowing what these metrics are measuring and how to interpret them.

The VMkernel maps guest physical memory to machine memory, but they are not always mapped one-to-one. Multiple regions of guest physical memory might be mapped to the same region of machine memory (when memory sharing) or specific regions of guest physical memory might not be mapped to machine memory (when the VMkernel swaps out or balloons guest physical memory). In these situations, calculations of guest physical memory usage and machine memory usage for an individual virtual machine or a host differ.

Consider the example in the following figure, which shows two virtual machines running on a host. Each block represents 4 KB of memory and each color/letter represents a different set of data on a block.

Figure 99: Memory Usage Example



The performance metrics for the virtual machines can be determined as follows:

- To determine Memory Granted (the amount of guest physical memory that is mapped to machine memory) for virtual machine 1, count the number of blocks in virtual machine 1's guest physical memory that have arrows to machine memory and multiply by 4 KB. Since there are five blocks with arrows, Memory Granted is 20 KB.
- Memory Consumed is the amount of machine memory allocated to the virtual machine, accounting for savings from shared memory. First, count the number of blocks in machine memory that have arrows from virtual machine 1's guest physical memory. There are three such blocks, but one block is shared with virtual machine 2. So count two full blocks plus half of the third and multiply by 4 KB for a total of 10 KB Memory Consumed.

The important difference between these two metrics is that Memory Granted counts the number of blocks with arrows at the guest physical memory level and Memory Consumed counts the number of blocks with arrows at the machine memory level. The number of blocks differs between the two levels due to memory sharing and so Memory Granted and Memory Consumed differ. Memory is being saved through sharing or other reclamation techniques.

A similar result is obtained when determining Memory Shared and Memory Shared Common for the host.

- Memory Shared for the host is the sum of each virtual machine's Memory Shared. Calculate shared memory by looking at each virtual machine's guest physical memory and counting the number of blocks that have arrows to machine memory blocks that themselves have more than one arrow pointing at them. There are six such blocks in the example, so Memory Shared for the host is 24 KB.

- Memory Shared Common is the amount of machine memory shared by virtual machines. To determine common memory, look at the machine memory and count the number of blocks that have more than one arrow pointing at them. There are three such blocks, so Memory Shared Common is 12 KB.

Memory Shared is concerned with guest physical memory and looks at the origin of the arrows. Memory Shared Common, however, deals with machine memory and looks at the destination of the arrows.

The memory metrics that measure guest physical memory and machine memory might appear contradictory. In fact, they are measuring different aspects of a virtual machine's memory usage. By understanding the differences between these metrics, you can better use them to diagnose performance issues.

Memory Reliability

Memory reliability, also known as error isolation, allows ESXi to stop using parts of memory when it determines that a failure might occur, as well as when a failure did occur.

When enough corrected errors are reported at a particular address, ESXi stops using this address to prevent the corrected error from becoming an uncorrected error.

Memory reliability provides better VMkernel reliability despite corrected and uncorrected errors in RAM. It also enables the system to avoid using memory pages that might contain errors.

Correcting an Error Isolation Notification

With memory reliability, VMkernel stops using pages that receive an error isolation notification.

The user receives an event in the vSphere Client when VMkernel recovers from an uncorrectable memory error, when VMkernel retires a significant percentage of system memory due to a large number of correctable errors, or if there are a large number of pages that are unable to retire.

1. Vacate the host.
2. Migrate the virtual machines.
3. Run memory related hardware tests.

About System Swap

System swap is a memory reclamation process that can take advantage of unused memory resources across an entire system.

System swap allows the system to reclaim memory from memory consumers that are not virtual machines. When system swap is enabled you have a tradeoff between the impact of reclaiming the memory from another process and the ability to assign the memory to a virtual machine that can use it. The amount of space required for the system swap is 1GB.

Memory is reclaimed by taking data out of memory and writing it to background storage. Accessing the data from background storage is slower than accessing data from memory, so it is important to carefully select where to store the swapped data.

ESXi determines automatically where the system swap should be stored, this is the **Preferred swap file location**. This decision can be aided by selecting a certain set of options. The system selects the best possible enabled option. If none of the options are feasible then system swap is not activated.

The available options are:

- Datastore - Allow the use of the datastore specified. Please note that a vSAN datastore or a VMware vSphere® Virtual VolumesTM datastore cannot be specified for system swap files.
- Host Swap Cache - Allow the use of part of the host swap cache.
- Preferred swap file location - Allow the use of the preferred swap file location configured for the host.

Configure System Swap

You can customize the options that determine the system swap location.

Select the **Enabled** check box in the **Edit System Swap Settings** dialog box.

1. Browse to the host in the vSphere Client.
2. Click **Configure**.
3. Under **System**, select **System Swap**.
4. Click **Edit**.
5. Select the check boxes for each option that you want to enable.
6. If you select the **datastore** option, select a datastore from the drop-down menu.
7. Click **OK**.

Persistent Memory

Persistent Memory (PMem), also known as Non-Volatile Memory (NVM), is capable of maintaining data even after a power outage. PMem can be used by applications that are sensitive to downtime and require high performance.

VMs can be configured to use PMem on a standalone host, or in a cluster. PMem is treated as a local datastore. Persistent memory significantly reduces storage latency. In ESXi you can create VMs that are configured with PMem, and applications inside these VMs can take advantage of this increased speed. Once a VM is initially powered on, PMem is reserved for it regardless of whether it is powered on or off. This PMem stays reserved until the VM is migrated or removed.

Persistent memory can be consumed by virtual machines in two different modes. Legacy guest OSes can still take advantage of virtual persistent memory disk feature.

- **Virtual Persistent Memory (vPMem)**
  Using vPMem, the memory is exposed to a guest OS as a virtual NVDIMM. This enables the guest OS to use PMem in byte addressable random mode.

  Note: You must use VM hardware version 14 and a guest OS that supports NVM technology.

  Note: You must use VM hardware version 19 when you configure vSphere HA for PMem VMs. For more information, see Configure vSphere HA for PMem VMs.
- **Virtual Persistent Memory Disk (vPMemDisk)**
  Using vPMemDisk, the memory can be accessed by the guest OS as a virtual SCSI device, but the virtual disk is stored in a PMem datastore.

When you create a VM with PMem, memory is reserved for it at the time of Hard disk creation. Admission control is also done at the time of Hard disk creation. For more information, see vSphere HA Admission Control PMem Reservation.

In a cluster, each VM has some capacity for PMem. The total amount of PMem must not be greater than the total amount available in the cluster. The consumption of PMem includes both powered on and powered off VMs. If a VM is configured to use PMem and you do not use DRS, then you must manually pick a host that has sufficient PMem to place the VM on.

NVDIMM and traditional storage

NVDIMM is accessed as memory. When you use traditional storage, software exists between applications and storage devices which can cause a delay in processing time. When you use PMem, the applications use the storage directly. This means that PMem performance is better than traditional storage. Storage is local to the host. However, since system software cannot track the changes, solutions such as backups do not currently work with PMem.

Solutions such as vSphere HA have limited scope if vPMem is used in a mode that is not write-through to a non-PMem datastore. When vSphere HA is activated for vPMem VMs with failover enabled, the VM can be failed over to different

host. When this happens, the VM is using the PMem resources on the new host. To free up the resources on the old host, a garbage collector periodically identifies and frees up these resources for use by other VMs.

Name spaces

Name spaces for PMem are configured before ESXi starts. Name spaces are similar to disks on the system. ESXi reads name spaces and combines multiple name spaces into one logical volume by writing GPT headers. This is formatted automatically by default, if you have not previously configured it. If it has already been formatted, ESXi attempts to mount the PMem.

GPT tables

If the data in PMem storage is corrupted it can cause ESXi to fail. To avoid this, ESXi checks for errors in the metadata during PMem mount time.

PMem regions

PMem regions are a continuous byte stream that represent a single vNVDimm or vPMemDisk. Each PMem volume belongs to a single host. This could be difficult to manage if an administrator has to manage each host in a cluster with a large number of hosts. However, you do not have to manage each individual datastore. Instead you can think of the entire PMem capacity in the cluster as one datastore.

VC and DRS automate initial placement of PMem datastores. Select a local PMem storage profile when the VM is created or when the device is added to the VM. The rest of the configuration is automated. One limitation is that ESXi does not allow you to put the VM home on a PMem datastore. This is because it takes up valuable space to store VM log and stat files. These regions are used to represent the VM data and can be exposed as byte addressable nvDimms, or VpMem disks.

Migration

Since PMem is a local datastore, if you want to move a VM you must use storage vMotion. A VM with vPMem can only be migrated to an ESX host with PMem resource. A VM with vPMemDisk can be migrated to an ESX host without a PMem resource.

Error handling and NVDimm management

Host failures can result in a loss of availability on vPMem VMs which are not in write-through mode. In the case of catastrophic errors, you may lose all data and must take manual steps to reformat the PMem.

vSphere Persistent Memory with the vSphere Client

For a brief conceptual introduction to Persistent Memory, see:

Enhancements to Working with PMEM in the vSphere Client

For a brief overview of enhancements in the HTML5-based vSphere Client when working with PMem, see:

Migrating and Cloning VMs Using PMEM in the vSphere Client

For a brief overview of migrating and cloning virtual machines that use PMem, see:

Configure vSphere HA for PMem VMs

You can configure vSphere HA for PMem VMs in write-through mode, so that when a host fails VMs can be restored on another functioning host.

- You must select Hardware version 19.

- PMem VMs with vPMemDisks are not supported.

1. When creating a new VM in the **New Virtual Machine** wizard, select **Customize hardware**.
   a) Click **ADD NEW DEVICE** and select **Add NVDIMM** from the drop-down menu.
   b) Click the checkbox **Allow failover on another host for all NVDIMM devices**.
   c) Click **NEXT** and complete the **New Virtual Machine** wizard.

      On Host failure, NVDIMM PMem data cannot be recovered. By default, HA will not attempt to restart this virtual machine on another host. Allowing HA on host failure to failover the virtual machine, will restart the virtual machine on another host with a new, empty NVDIMM.
2. To enable HA on an existing VM, browse to the VM.
   a) Under **VM Hardware**, click **EDIT**.
   b) Select the NVDIMM.
   c) Click the checkbox **Allow failover on another host for all NVDIMM devices**.
   d) Click **OK**.

      On host failure, HA will restart this virtual machine on another host with new, empty NVDIMMs.

vSphere HA Admission Control PMem Reservation

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster.

Raising the number of potential host failures to tolerate will increase the availability restraints and capacity reserved. You can reserve a percentage of Persistent Memory for Host failover capacity. This is actual storage capacity that is blocked and must be considered for host power off.

Under **Edit Cluster Settings** you can select **Admission Control** to specify the number of failures the host will tolerate.

If you select CPU/Memory reservation defined by:

- **Cluster resource percentage**, some amount of persistent memory capacity in the cluster is dedicated for failover purpose even if the virtual machines in the cluster are not using persistent memory currently. This percentage can either be specified through an override, or it is automatically calculated according to the **host failures to tolerate** setting. When PMem admission control is enabled, PMem capacity is reserved across the cluster even if there are VMs using PMem as disks.
- **Slot Policy (powered-on VMs)**, persistent memory admission control overrides the Slot Policy with the Cluster Resource Percentage policy, for persistent memory resources only. The percentage value is automatically calculated from the **host failures cluster tolerates** setting and cannot be overriden.
- **Dedicated failover hosts**, the persistent memory of the dedicated failover hosts is dedicated for failover purpose and you cannot provision virtual machines with persistent memory on these hosts.

Note: After you select an admission control policy, you must also click the **Reserve Persistent Memory failover capacity** checkbox to enable PMem admission control.

vSphere Memory Monitoring and Remediation

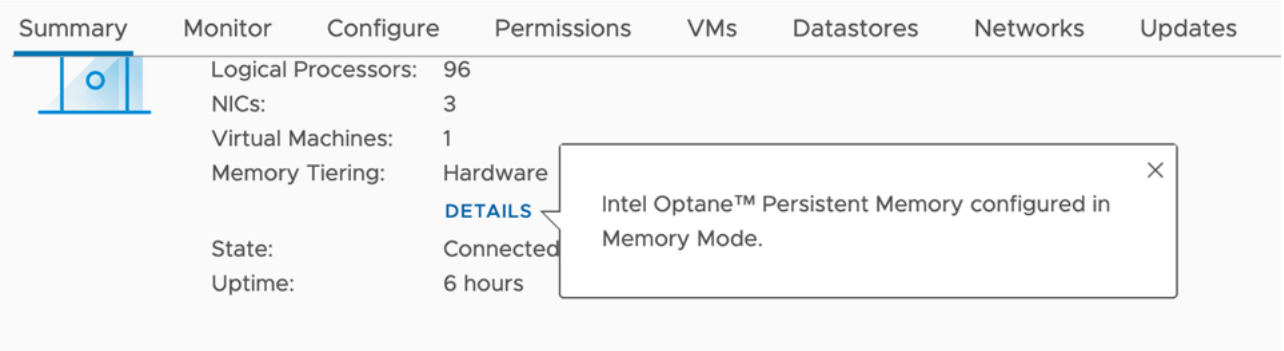
vMMR collects data and provides visibility of performance statistics so you can determine if your application workload is regressed due to Memory Mode.

Intel Optane Persistent Memory can be configured in BIOS settings in App Direct or Memory Mode. In App Direct mode, persistent memory can be accessed as byte addressable, persistent memory along with DRAM. In Memory Mode, DRAM becomes the hardware cache and the larger PMem becomes volatile and appears as system memory.

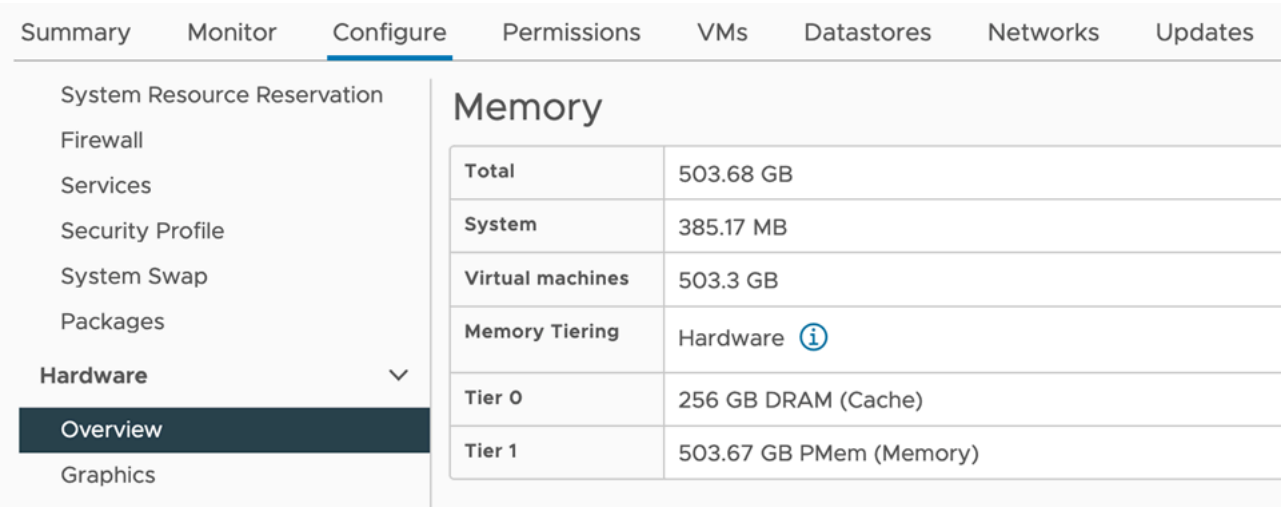
Memory Mode is invisible and transparent to VMs. Once you configure the system in Memory Mode, the system appears as a traditional system with DRAM. A cluster can have a mix of hosts with different configurations. vSphere shows additional information about the system being in Memory Mode. ESXi programs performance counters that gather

information about host level and VM level statistics. These performance statistics are used to create alarms. Statistics are also tracked in performance charts.

You can find out if the system is in Memory Mode in the host **Summary** tab, **Memory Tiering: Hardware with some additional details**.



You can also view the size of DRAM and PMEM under **Configure** > **Hardware** > **Overview** > **Memory**.



ESXi gathers and exposes two kinds of memory statistics:

- Host Level Statistics: A memory sub-component measures DRAM and PMem performance by programming performance counters. The host level statistics are total, read/write bandwidth, read/write latency and miss rate for the different memory types (DRAM, PMem).
- VM Level Statistics: vSphere monitors performance counters to get data on DRAM and PMEM read bandwidth of the VM.

Both Host and VM have new Memory pane under Performance charts. This shows memory details like Memory Utilization and Memory Reclamation along with new statistics. On the ESXi host level, you can monitor the Memory Bandwidth and Memory Miss Rate charts. On the VM level, you can view the PMem read bandwidth and DRAM read bandwidth.

From the **VMs** tab of an ESXi host, you can view a list containing performance information about all virtual machines that reside on the host. To display information about the Memory Mode impact on a virtual machine, click the view columns ( ) icon and select the Active Memory, DRAM Read Bandwidth, and PMem Read Bandwidth metrices.

There are two preconfigured default alarms, one at the host level (Host Memory Mode High Active DRAM Usage) and another at the VM level (Virtual Machine High PMem Bandwidth Usage). If the alarm condition is met, an event will be

published to trigger the corresponding alarm. You can also create custom alarms based on performance metrics. vMMR alarms only work on hosts configured with Memory Mode.

When DRS is enabled and fully automated in the cluster, if the active memory utilization of the host is above certain percentage of the size of the DRAM cache, DRS might move some VMs out of the host in order to balance the load.

For more information, see *vSphere Monitoring and Performance*.

Note: vMMR is supported on Intel Broadwell, Skylake, Cascade Lake and Ice Lake platforms. Host Level DRAM statistics are available on these platforms. Host and VM Level PMem statistics are only available in Cascade Lake and Ice Lake hosts configured in Memory Mode.

Configuring Virtual Graphics

You can edit graphics settings for supported graphics implementations.

vSphere supports multiple graphics implementations.

- VMware supports 3d graphics solutions from AMD, Intel and NVIDIA.
- NVIDIA GRID support.
- Allows single NVIDIA vib to support both vSGA and vGPU implementations.
- Provides vCenter GPU performance charts for Intel and NVIDIA.
- Enables graphics for Horizon View VDI desktops.

You can configure host graphics settings, and customize vGPU graphics settings on a per VM basis.

Note: In this chapter, "Memory" refers to physical RAM.

View GPU Statistics

You can view detailed information for a host graphics card.

You can see GPU temperature, utilization, and memory usage.

Note: These statistics are only displayed when the GPU driver is installed on the host.

1. In the vSphere Client, navigate to the host.
2. Click the **Monitor** tab and click **Performance**.
3. Click **Advanced** and select **GPU** from the drop-down menu.

Add an NVIDIA GRID vGPU to a Virtual Machine

If an ESXi host has an NVIDIA GRID GPU graphics device, you can configure a virtual machine to use the NVIDIA GRID virtual GPU (vGPU) technology.

- Verify that an NVIDIA GRID GPU graphics device with an appropriate driver is installed on the host. See the *vSphere Upgrade* documentation.
- Verify that the virtual machine is compatible with ESXi 6.0 and later.

NVIDIA GRID GPU graphics devices are designed to optimize complex graphics operations and enable them to run at high performance without overloading the CPU.

1. Right-click a virtual machine and select **Edit Settings**.
2. On the **Virtual Hardware** tab, select **Add New Device** and select **New PCI Device** from the drop-down menu.
3. Expand the **New PCI device**, and select the NVIDIA GRID vGPU passthrough device to which to connect your virtual machine.

   Note: Full memory reservation will be applied automatically, it's required for PCI device.

4. Select a GPU profile.
   A GPU profile represents the vGPU type.
5. Click **OK**.

The virtual machine can access the device.

Configuring Host Graphics

You can customize the graphics options on a per host basis.

Virtual machines should be powered off.

1. Select a host and select **Configure** > **Graphics**.
2. Under **Host Graphics**, select **Edit**.
3. In the **Edit Host Graphics Settings** window, select:

Option	Description
Shared	VMware shared virtual graphics
Shared Direct	Vendor shared passthrough graphics

4. Select a shared passthrough GPU assignment policy.
   a) Spread VMs across GPUs (best performance)
   b) Group VMs on GPU until full (GPU Consolidation)
5. Click **OK**.

After clicking **OK**, you must restart Xorg on the host.

Configuring Graphics Devices

You can edit graphics type for a video card.

Virtual machines must be powered off.

1. Under **Graphics Devices**, select a graphics card and click **Edit**.
   a) Select **Shared** for VMware shared virtual graphics.
   b) Select **Shared Direct** for Vendor shared passthrough graphics.
2. Click **OK**.

If you select a device, it shows which virtual machines are using that device if they are active.

After clicking **OK**, you must restart Xorg on the host.

Managing Storage I/O Resources

vSphere Storage I/O Control allows cluster-wide storage I/O prioritization, which allows better workload consolidation and helps reduce extra costs associated with over provisioning.

Storage I/O Control extends the constructs of shares and limits to handle storage I/O resources. You can control the amount of storage I/O that is allocated to virtual machines during periods of I/O congestion, which ensures that more important virtual machines get preference over less important virtual machines for I/O resource allocation.

When you enable Storage I/O Control on a datastore, ESXi begins to monitor the device latency that hosts observe when communicating with that datastore. When device latency exceeds a threshold, the datastore is considered to be congested and each virtual machine that accesses that datastore is allocated I/O resources in proportion to their shares. You set shares per virtual machine. You can adjust the number for each based on need.

The I/O filter framework (VAIO) allows VMware and its partners to develop filters that intercept I/O for each VMDK and provides the desired functionality at the VMDK granularity. VAIO works along Storage Policy-Based Management (SPBM) which allows you to set the filter preferences through a storage policy that is attached to VMDKs.

Configuring Storage I/O Control is a two-step process:

1. Enable Storage I/O Control for the datastore.
2. Set the number of storage I/O shares and upper limit of I/O operations per second (IOPS) allowed for each virtual machine.

By default, all virtual machine shares are set to Normal (1000) with unlimited IOPS.

Note: Storage I/O Control is enabled by default on Storage DRS-enabled datastore clusters.

Note: In this chapter, "Memory" refers to physical RAM.

About Virtual Machine Storage Policies

Virtual machine storage policies are essential to virtual machine provisioning. The policies control which type of storage is provided for the virtual machine, how the virtual machine is placed within the storage, and which data services are offered for the virtual machine.

vSphere includes default storage policies. However, you can define and assign new policies.

You use the VM Storage Policies interface to create a storage policy. When you define the policy, you specify various storage requirements for applications that run on virtual machines. You can also use storage policies to request specific data services, such as caching or replication, for virtual disks.

You apply the storage policy when you create, clone, or migrate the virtual machine. After you apply the storage policy, the Storage Policy Based Management (SPBM) mechanism places the virtual machine in a matching datastore and, in certain storage environments, determines how the virtual machine storage objects are provisioned and allocated within the storage resource to guarantee the required level of service. The SPBM also enables requested data services for the virtual machine. vCenter Server monitors policy compliance and sends an alert if the virtual machine is in breach of the assigned storage policy.

See *vSphere Storage* for more information.

About I/O Filters

I/O filters that are associated with virtual disks gain direct access to the virtual machine I/O path regardless of the underlying storage topology.

VMware offers certain categories of I/O filters. In addition, the I/O filters can be created by third-party vendors. Typically, they are distributed as packages that provide an installer to deploy filter components on vCenter Server and ESXi host clusters.

When I/O filters are deployed on the ESXi cluster, vCenter Server automatically configures and registers an I/O filter storage provider, also called a VASA provider, for each host in the cluster. The storage providers communicate with vCenter Server and make data services offered by the I/O filter visible in the VM Storage Policies interface. You can reference these data services when defining common rules for a VM policy. After you associate virtual disks with this policy, the I/O filters are enabled on the virtual disks.

See *vSphere Storage* for more information.

Storage I/O Control Requirements

Storage I/O Control has several requirements and limitations.

- Datastores that are Storage I/O Control-enabled must be managed by a single vCenter Server system.

- Storage I/O Control is supported on Fibre Channel-connected, iSCSI-connected, and NFS-connected storage. Raw Device Mapping (RDM) is not supported.
- Storage I/O Control does not support datastores with multiple extents.
- Before using Storage I/O Control on datastores that are backed by arrays with automated storage tiering capabilities, check the *VMware Storage/SAN Compatibility Guide* to verify whether your automated tiered storage array has been certified to be compatible with Storage I/O Control.

  Automated storage tiering is the ability of an array (or group of arrays) to migrate LUNs/volumes or parts of LUNs/volumes to different types of storage media (SSD, FC, SAS, SATA) based on user-set policies and current I/O patterns. No special certification is required for arrays that do not have these automatic migration/tiering features, including those that provide the ability to manually migrate data between different types of storage media.

Storage I/O Control Resource Shares and Limits

You allocate the number of storage I/O shares and upper limit of I/O operations per second (IOPS) allowed for each virtual machine. When storage I/O congestion is detected for a datastore, the I/O workloads of the virtual machines accessing that datastore are adjusted according to the proportion of virtual machine shares each virtual machine has.

Storage I/O shares are similar to shares used for memory and CPU resource allocation, which are described in Resource Allocation Shares. These shares represent the relative importance of a virtual machine regarding the distribution of storage I/O resources. Under resource contention, virtual machines with higher share values have greater access to the storage array. When you allocate storage I/O resources, you can limit the IOPS allowed for a virtual machine. By default, IOPS are unlimited.

The benefits and drawbacks of setting resource limits are described in Resource Allocation Limit. If the limit you want to set for a virtual machine is in terms of MB per second instead of IOPS, you can convert MB per second into IOPS based on the typical I/O size for that virtual machine. For example, to restrict a back up application with 64 KB IOs to 10 MB per second, set a limit of 160 IOPS.

View Storage I/O Control Shares and Limits

You can view the shares and limits for all virtual machines running on a datastore. Viewing this information allows you to compare the settings of all virtual machines that are accessing the datastore, regardless of the cluster in which they are running.

1. Browse to the datastore in the vSphere Client.
2. Click the **VMs** tab.

   The tab displays each virtual machine running on the datastore and the associated shares value, and percentage of datastore shares.

Monitor Storage I/O Control Shares

Use the datastore **Performance** tab to monitor how Storage I/O Control handles the I/O workloads of the virtual machines accessing a datastore based on their shares.

Datastore performance charts allow you to monitor the following information:

- Average latency and aggregated IOPS on the datastore
- Latency among hosts
- Queue depth among hosts
- Read/write IOPS among hosts
- Read/write latency among virtual machine disks

- Read/write IOPS among virtual machine disks

1. Browse to the datastore in the vSphere Client.
2. Under the **Monitor** tab, click **Performance**.
3. Select **Advanced**.

Set Storage I/O Control Resource Shares and Limits

Allocate storage I/O resources to virtual machines based on importance by assigning a relative amount of shares to the virtual machine.

See *vSphere Storage* for information on creating VM storage policies and defining common rules for VM storage policies.

Unless virtual machine workloads are very similar, shares do not necessarily dictate allocation in terms of I/O operations or megabytes per second. Higher shares allow a virtual machine to keep more concurrent I/O operations pending at the storage device or datastore compared to a virtual machine with lower shares. Two virtual machines might experience different throughput based on their workloads.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and click **Edit Settings**.
3. Click the **Virtual Hardware** tab and select a virtual hard disk from the list. Expand **Hard disk**.
4. Select a **VM storage policy** from the drop-down menu.
   If you select a storage policy, do not manually configure **Shares** and **Limit - IOPS**.
5. Under **Shares**, click the drop-down menu and select the relative amount of shares to allocate to the virtual machine (Low, Normal, or High).
   You can select **Custom** to enter a user-defined shares value.
6. Under **Limit - IOPS**, click the drop-down menu and enter the upper limit of storage resources to allocate to the virtual machine.
   IOPS are the number of I/O operations per second. By default, IOPS are unlimited. You select Low (500), Normal (1000), or High (2000), or you can select Custom to enter a user-defined number of shares.
7. Click **OK**.

Enable Storage I/O Control

When you enable Storage I/O Control, ESXi monitors datastore latency and throttles the I/O load if the datastore average latency exceeds the threshold.

1. Browse to the datastore in the vSphere Client.
2. Click the **Configure** tab.
3. Click **Settings** and click **General**.
4. Click **Edit** for **Datastore Capabilities**.
5. Select the **Enable Storage I/O Control** check box.
6. Click **OK**.

Under **Datastore Capabilities**, Storage I/O Control is enabled for the datastore.

Set Storage I/O Control Threshold Value

The congestion threshold value for a datastore is the upper limit of latency that is allowed for a datastore before Storage I/O Control begins to assign importance to the virtual machine workloads according to their shares.

Verify that Storage I/O Control is enabled.

You do not need to adjust the threshold setting in most environments.
CAUTION: Storage I/O Control might not function correctly if you share the same spindles on two different datastores.

If you change the congestion threshold setting, set the value based on the following considerations.

- A higher value typically results in higher aggregate throughput and weaker isolation. Throttling will not occur unless the overall average latency is higher than the threshold.
- If throughput is more critical than latency, do not set the value too low. For example, for Fibre Channel disks, a value below 20ms could lower peak disk throughput. A very high value (above 50ms) might allow very high latency without any significant gain in overall throughput.
- A lower value will result in lower device latency and stronger virtual machine I/O performance isolation. Stronger isolation means that the shares controls are enforced more often. Lower device latency translates into lower I/O latency for the virtual machines with the highest shares, at the cost of higher I/O latency experienced by the virtual machines with fewer shares.
- A very low value (lower than 20ms) will result in lower device latency and isolation among I/Os at the potential cost of a decrease in aggregate datastore throughput.
- Setting the value extremely high or extremely lowly results in poor isolation.

1. Browse to the datastore in the vSphere Client.
2. Click the **Configure** tab and click **Settings**.
3. Click **General**.
4. Click **Edit** for **Datastore Capabilities**.
5. Select the **Enable Storage I/O Control** check box.

   Storage I/O Control automatically sets the latency threshold that corresponds to the estimated latency when the datastore is operating at 90% of its peak throughput.
6. Optional: Adjust the **Congestion Threshold**.

   - Select a value from the **Percentage of peak throughput** drop-down menu.

   The percentage of peak throughput value indicates the estimated latency threshold when the datastore is using that percentage of its estimated peak throughput.

   - Select a value from the **Manual** drop-down menu.

   The value must be between 5ms and 100ms. Setting improper congestion threshold values can be detrimental to the performance of the virtual machines on the datastore.
7. Optional: Click **Reset to defaults** to restore the congestion threshold setting to the default value (30ms).
8. Click **OK**.

Storage DRS Integration with Storage Profiles

Storage Policy Based Management (SPBM) allows you to specify the policy for a virtual machine which is enforced by Storage DRS. A datastore cluster can have set of datastores with different capability profiles. If the virtual machines have storage profiles associated with them, Storage DRS can enforce placement based on underlying datastore capabilities.

By default, Storage DRS will not enforce storage policies associated with a virtual machine. Please configure `EnforceStorageProfiles` option according to your requirements. The options are Default (0), Soft (1) or Hard (2).

As part of Storage DRS integration with storage profiles, the Storage DRS cluster level advanced option `EnforceStorageProfiles` is introduced. Advanced option `EnforceStorageProfiles` takes one of these integer values: 0,1 or 2. The default value is 0. When the option is set to 0, it indicates that there is no storage profile or policy enforcement on the Storage DRS cluster. When the option is set to 1, it indicates that there is a storage profile or policy soft enforcement on the Storage DRS cluster. This is analogous with DRS soft rules. Storage DRS will comply with storage profile or policy in the optimum level. Storage DRS will violate the storage profile compliant if it is required to do so. Storage DRS affinity rules will have higher precedence over storage profiles only when storage profile enforcement is set to 1. When the option is set to 2, it indicates that there is a storage profile or policy hard enforcement on the Storage DRS cluster. This is analogous with DRS hard rules. Storage DRS will not violate the storage profile or policy compliant. Storage profiles will have higher precedence over affinity rules. Storage DRS will generate fault: `could not fix anti-affinity rule violation`

1. Log in to the vSphere Client as an Administrator.
2. In the vSphere Client, click on the Storage DRS cluster, then select **Manage** > **Settings** > **Storage DRS**.
3. Click **Edit** > **Advanced Options** > **Configuration parameters** and select **Add**.
4. Click in the area under the Option heading and type `EnforceStorageProfiles`
5. Click in the area under the Value heading to the right of the previously entered advanced option name and type the value of either 0, 1 or 2.
6. Click **OK**.

Managing Resource Pools

A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources.

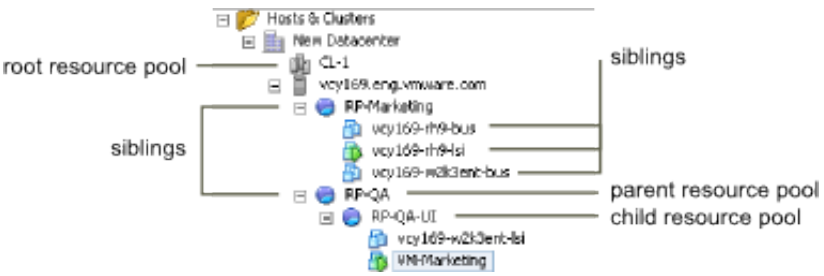
Each standalone host and each DRS cluster has an (invisible) root resource pool that groups the resources of that host or cluster. The root resource pool does not appear because the resources of the host (or cluster) and the root resource pool are always the same.

Users can create child resource pools of the root resource pool or of any user-created child resource pool. Each child resource pool owns some of the parent's resources and can, in turn, have a hierarchy of child resource pools to represent successively smaller units of computational capability.

A resource pool can contain child resource pools, virtual machines, or both. You can create a hierarchy of shared resources. The resource pools at a higher level are called parent resource pools. Resource pools and virtual machines that are at the same level are called siblings. The cluster itself represents the root resource pool. If you do not create child resource pools, only the root resource pools exist.

In the following example, RP-QA is the parent resource pool for RP-QA-UI. RP-Marketing and RP-QA are siblings. The three virtual machines immediately below RP-Marketing are also siblings.

Figure 100: Parents, Children, and Siblings in Resource Pool Hierarchy



For each resource pool, you specify reservation, limit, shares, and whether the reservation should be expandable. The resource pool resources are then available to child resource pools and virtual machines.

Note: In this chapter, "Memory" refers to physical RAM.

Why Use Resource Pools?

Resource pools allow you to delegate control over resources of a host (or a cluster), but the benefits are evident when you use resource pools to compartmentalize all resources in a cluster. Create multiple resource pools as direct children of the host or cluster and configure them. You can then delegate control over the resource pools to other individuals or organizations.

Using resource pools can result in the following benefits.

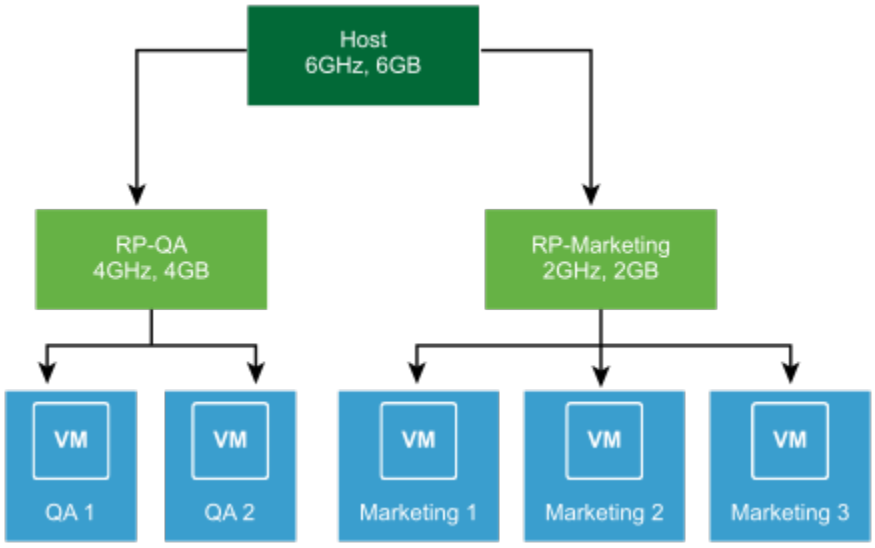
- Flexible hierarchical organization—Add, remove, or reorganize resource pools or change resource allocations as needed.
- Isolation between pools, sharing within pools—Top-level administrators can make a pool of resources available to a department-level administrator. Allocation changes that are internal to one departmental resource pool do not unfairly affect other unrelated resource pools.
- Access control and delegation—When a top-level administrator makes a resource pool available to a department-level administrator, that administrator can then perform all virtual machine creation and management within the boundaries of the resources to which the resource pool is entitled by the current shares, reservation, and limit settings. Delegation is usually done in conjunction with permissions settings.
- Separation of resources from hardware—If you are using clusters enabled for DRS, the resources of all hosts are always assigned to the cluster. That means administrators can perform resource management independently of the actual hosts that contribute to the resources. If you replace three 2GB hosts with two 3GB hosts, you do not need to make changes to your resource allocations.

  This separation allows administrators to think more about aggregate computing capacity and less about individual hosts.
- Management of sets of virtual machines running a multitier service— Group virtual machines for a multitier service in a resource pool. You do not need to set resources on each virtual machine. Instead, you can control the aggregate allocation of resources to the set of virtual machines by changing settings on their enclosing resource pool.

For example, assume a host has a number of virtual machines. The marketing department uses three of the virtual machines and the QA department uses two virtual machines. Because the QA department needs larger amounts of CPU and memory, the administrator creates one resource pool for each group. The administrator sets **CPU Shares** to **High** for the QA department pool and to **Normal** for the Marketing department pool so that the QA department users can run automated tests. The second resource pool with fewer CPU and memory resources is sufficient for the lighter load of the marketing staff. Whenever the QA department is not fully using its allocation, the marketing department can use the available resources.

The numbers in the following figure show the effective allocations to the resource pools.

Figure 101: Allocating Resources to Resource Pools



Create a Resource Pool

You can create a child resource pool of any ESXi host, resource pool, or DRS cluster.

The vSphere Client is connected to the vCenter Server system.

Note: If a host has been added to a cluster, you cannot create child resource pools of that host. If the cluster is enabled for DRS, you can create child resource pools of the cluster.

When you create a child resource pool, you are prompted for resource pool attribute information. The system uses admission control to make sure you cannot allocate resources that are not available. If you want your shares to scale dynamically when adding or removing VMs, you can select scalable shares.

Note: Shares are scaled at the parent level. All descendant resource pools created from a parent with scalable shares have scalable shares by default.

1. In the vSphere Client, select a parent object for the resource pool (a host, another resource pool, or a DRS cluster).
2. Right-click the object and select **New Resource Pool**.
3. Type a name to identify the resource pool.
4. Select the checkbox if you want to enable scalable shares.
5. Specify how to allocate CPU and memory resources.

   The CPU resources for your resource pool are the guaranteed physical resources the host reserves for a resource pool. Normally, you accept the default and let the host handle resource allocation.

Option	Description
Shares	Specify shares for this resource pool with respect to the parent's total resources. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit. • Select **Low**, **Normal**, or **High** to specify share values respectively in a 1:2:4 ratio. • Select **Custom** to give each virtual machine a specific number of shares, which expresses a proportional weight.
Reservation	Specify a guaranteed CPU or memory allocation for this resource pool. Defaults to 0.

Option	Description
	A nonzero reservation is subtracted from the unreserved resources of the parent (host or resource pool). The resources are considered reserved, regardless of whether virtual machines are associated with the resource pool.
Expandable Reservation	When the check box is selected (default), expandable reservations are considered during admission control. If you power on a virtual machine in this resource pool, and the combined reservations of the virtual machines are larger than the reservation of the resource pool, the resource pool can use resources from its parent or ancestors.
Limit	Specify the upper limit for this resource pool's CPU or memory allocation. You can usually accept the default (**Unlimited**). To specify a limit, deselect the **Unlimited** check box.

6. Click **OK**.

After you create a resource pool, you can add virtual machines to it. A virtual machine's shares are relative to other virtual machines (or resource pools) with the same parent resource pool.

Creating Resource Pools

Assume that you have a host that provides 6GHz of CPU and 3GB of memory that must be shared between your marketing and QA departments. You also want to share the resources unevenly, giving one department (QA) a higher priority. This can be accomplished by creating a resource pool for each department and using the **Shares** attribute to prioritize the allocation of resources.

The example shows how to create a resource pool with the ESXi host as the parent resource.

1. In the **New Resource Pool** dialog box, type a name for the QA department's resource pool (for example, RP-QA).
2. Specify **Shares** of **High** for the CPU and memory resources of RP-QA.
3. Create a second resource pool, RP-Marketing.
   Leave Shares at **Normal** for CPU and memory.
4. Click **OK**.

If there is resource contention, RP-QA receives 4GHz and 2GB of memory, and RP-Marketing 2GHz and 1GB. Otherwise, they can receive more than this allotment. Those resources are then available to the virtual machines in the respective resource pools.

Related Links

Add a Virtual Machine to a Resource Pool on page 3015

When you create a virtual machine, you can specify a resource pool location as part of the creation process. You can also add an existing virtual machine to a resource pool.

Edit a Resource Pool

After you create the resource pool, you can edit its CPU and memory resource settings.

1. Browse to the resource pool in the vSphere Client.
2. Select **Edit Resource Settings** from the **Actions** drop-down menu.
3. Optional: You can change all attributes of the selected resource pool as described in Create a Resource Pool.
   - Select the checkbox if you want to enable sclalable shares.

     Note: Shares are scaled at the parent level. All descendant resource pools created from a parent with scalable shares have scalable shares by default.
   - Under **CPU**, select CPU resource settings.
   - Under **Memory**, select memory resource settings.
4. Click **OK** to save your changes.

Add a Virtual Machine to a Resource Pool

When you create a virtual machine, you can specify a resource pool location as part of the creation process. You can also add an existing virtual machine to a resource pool.

When you move a virtual machine to a new resource pool:

- The virtual machine's reservation and limit do not change.
- If the virtual machine's shares are high, medium, or low, %Shares adjusts to reflect the total number of shares in use in the new resource pool.
- If the virtual machine has custom shares assigned, the share value is maintained.

  Note: Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares when you move it into a resource pool so that the virtual machine's shares are consistent with the relative values in the new resource pool. A warning appears if a virtual machine would receive a very large (or very small) percentage of total shares.
- Under **Monitor**, the information displayed in the **Resource Reservation** tab about the resource pool's reserved and unreserved CPU and memory resources changes to reflect the reservations associated with the virtual machine (if any).

  Note: If a virtual machine has been powered off or suspended, it can be moved but overall available resources (such as reserved and unreserved CPU and memory) for the resource pool are not affected.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and click **Migrate**.
   - You can move the virtual machine to another host.
   - You can move the virtual machine's storage to another datastore.
   - You can move the virtual machine to another host and move its storage to another datastore.
3. Select a resource pool in which to run the virtual machine.
4. Review your selections and click **Finish**.

If a virtual machine is powered on, and the destination resource pool does not have enough CPU or memory to guarantee the virtual machine's reservation, the move fails because admission control does not allow it. An error dialog box displays available and requested resources, so you can consider whether an adjustment might resolve the issue.

Remove a Virtual Machine from a Resource Pool

You can remove a virtual machine from a resource pool either by moving the virtual machine to another resource pool or deleting it.

When you remove a virtual machine from a resource pool, the total number of shares associated with the resource pool decreases, so that each remaining share represents more resources. For example, assume you have a pool that is entitled to 6GHz, containing three virtual machines with shares set to **Normal**. Assuming the virtual machines are CPU-bound, each gets an equal allocation of 2GHz. If one of the virtual machines is moved to a different resource pool, the two remaining virtual machines each receive an equal allocation of 3GHz.

1. Browse to the resource pool in the vSphere Client.
2. Choose one of the following methods to remove the virtual machine from a resource pool.
   - Right-click the virtual machine and select **Move To...** to move the virtual machine to another resource pool.

     You do not need to power off the virtual machine before you move it.
   - Right-click the virtual machine and select **Delete from Disk**.

     You must power off the virtual machine before you can completely remove it.

Remove a Resource Pool

You can remove a resource pool from the inventory.

1. In the vSphere Client, right-click the resource pool and Select **Delete**.
   A confirmation dialog box appears.
2. Click **Yes** to remove the resource pool.

Resource Pool Admission Control

When you power on a virtual machine in a resource pool, or try to create a child resource pool, the system performs additional admission control to ensure the resource pool's restrictions are not violated.

Before you power on a virtual machine or create a resource pool, ensure that sufficient resources are available using the **Resource Reservation** tab in the vSphere Client. The **Available Reservation** value for CPU and memory displays resources that are unreserved.

How available CPU and memory resources are computed and whether actions are performed depends on the **Reservation Type**.

Table 331: Reservation Types

Reservation Type	Description
Fixed	The system checks whether the selected resource pool has sufficient unreserved resources. If it does, the action can be performed. If it does not, a message appears and the action cannot be performed.
Expandable (default)	The system considers the resources available in the selected resource pool and its direct parent resource pool. If the parent resource pool also has the **Expandable Reservation** option selected, it can borrow resources from its parent resource pool. Borrowing resources occurs recursively from the ancestors of the current resource pool as long as the **Expandable Reservation** option is selected. Leaving this option selected offers more flexibility, but, at the same time provides less protection. A child resource pool owner might reserve more resources than you anticipate.

The system does not allow you to violate preconfigured **Reservation** or **Limit** settings. Each time you reconfigure a resource pool or power on a virtual machine, the system validates all parameters so all service-level guarantees can still be met.

Expandable Reservations Example 1

This example shows you how a resource pool with expandable reservations works.

Assume an administrator manages pool P, and defines two child resource pools, S1 and S2, for two different users (or groups).

The administrator knows that users want to power on virtual machines with reservations, but does not know how much each user will need to reserve. Making the reservations for S1 and S2 expandable allows the administrator to more flexibly share and inherit the common reservation for pool P.

Without expandable reservations, the administrator needs to explicitly allocate S1 and S2 a specific amount. Such specific allocations can be inflexible, especially in deep resource pool hierarchies and can complicate setting reservations in the resource pool hierarchy.

Expandable reservations cause a loss of strict isolation. S1 can start using all of P's reservation, so that no memory or CPU is directly available to S2.

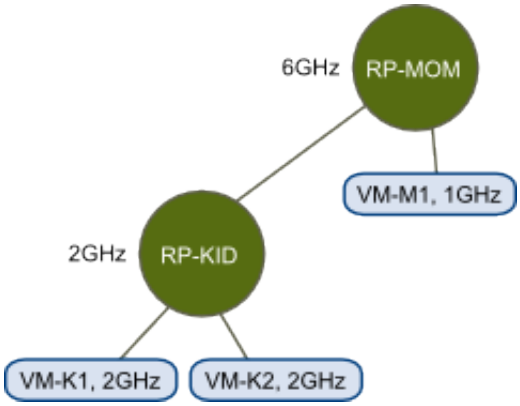
Expandable Reservations Example 2

This example shows how a resource pool with expandable reservations works.

Assume the following scenario, as shown in the figure.

- Parent pool RP-MOM has a reservation of 6GHz and one running virtual machine VM-M1 that reserves 1GHz.
- You create a child resource pool RP-KID with a reservation of 2GHz and with **Expandable Reservation** selected.
- You add two virtual machines, VM-K1 and VM-K2, with reservations of 2GHz each to the child resource pool and try to power them on.
- VM-K1 can reserve the resources directly from RP-KID (which has 2GHz).
- No local resources are available for VM-K2, so it borrows resources from the parent resource pool, RP-MOM. RP-MOM has 6GHz minus 1GHz (reserved by the virtual machine) minus 2GHz (reserved by RP-KID), which leaves 3GHz unreserved. With 3GHz available, you can power on the 2GHz virtual machine.

Figure 102: Admission Control with Expandable Resource Pools: Successful Power-On

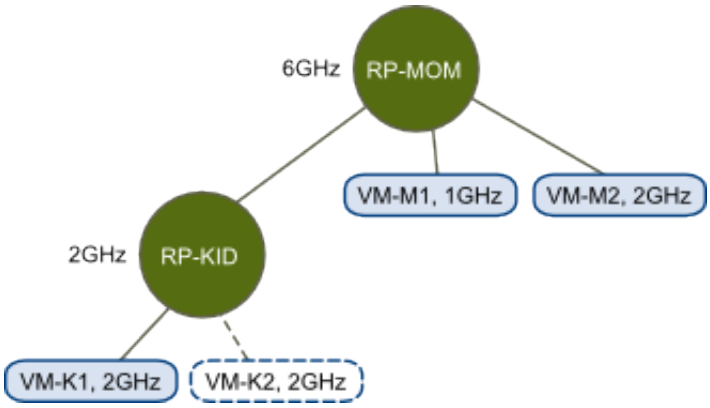


Now, consider another scenario with VM-M1 and VM-M2.

- Power on two virtual machines in RP-MOM with a total reservation of 3GHz.

- You can still power on VM-K1 in RP-KID because 2GHz are available locally.
- When you try to power on VM-K2, RP-KID has no unreserved CPU capacity so it checks its parent. RP-MOM has only 1GHz of unreserved capacity available (5GHz of RP-MOM are already in use—3GHz reserved by the local virtual machines and 2GHz reserved by RP-KID). As a result, you cannot power on VM-K2, which requires a 2GHz reservation.

Figure 103: Admission Control with Expandable Resource Pools: Power-On Prevented



Creating a DRS Cluster

A cluster is a collection of ESXi hosts and associated virtual machines with shared resources and a shared management interface. Before you can obtain the benefits of cluster-level resource management, you must create a cluster and activate DRS.

To fully leverage the benefits of DRS, such as DRS Load Balancing and DRS Initial Placement, the cluster must contain more than one host.

Depending on whether or not Enhanced vMotion Compatibility (EVC) is activated, DRS behaves differently when you use vSphere Fault Tolerance (vSphere FT) virtual machines in your cluster.

Table 332: DRS Behavior with vSphere FT Virtual Machines and EVC

EVC	DRS (Load Balancing)	DRS (Initial Placement)
Enabled	Enabled (Primary and Secondary VMs)	Enabled (Primary and Secondary VMs)
Disabled	Disabled (Primary and Secondary VMs)	Disabled (Primary VMs) Fully Automated (Secondary VMs)

vSphere Cluster Services

vSphere Cluster Services (vCLS) is activated by default and runs in all vSphere clusters. vCLS ensures that if vCenter Server becomes unavailable, cluster services remain available to maintain the resources and health of the workloads that run in the clusters. vCenter Server is still required to run DRS and HA.

vCLS is activated when you upgrade to vSphere 7.0 Update 3 or when you have a new vSphere 7.0 Update 3 deployment. vCLS is upgraded as part of vCenter Server upgrade.

vCLS uses agent virtual machines to maintain cluster services health. The vCLS agent virtual machines (vCLS VMs) are created when you add hosts to clusters. Up to three vCLS VMs are required to run in each vSphere cluster, distributed within a cluster. vCLS is also activated on clusters which contain only one or two hosts. In these clusters the number of vCLS VMs is one and two, respectively.

New anti-affinity rules are applied automatically. Every three minutes a check is performed, if multiple vCLS VMs are located on a single host they will be automatically redistributed to different hosts.

Table 333: Number of vCLS Agent VMs in Clusters

Number of Hosts in a Cluster	Number of vCLS Agent VMs
1	1
2	2
3 or more	3

vCLS VMs run in every cluster even if cluster services like vSphere DRS or vSphere HA are not activated on the cluster. The life cycle operations of vCLS VMs are managed by vCenter Server services like ESX Agent Manager and Workload Control Plane. vCLS VMs do not support NICs.

A cluster activated with vCLS can contain ESXi hosts of different versions if the ESXi versions are compatible with vCenter Server. vCLS works with vSphere Lifecycle Manager clusters.

vSphere DRS

vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere cluster. DRS depends on the availability of vCLS VMs.

Note: If you try to activate DRS on a cluster where there are issues with the vCLS VMs, a warning message is displayed on the **Cluster Summary** page.

Note: If DRS is on but there are issues with the vCLS VMs, you must resolve these issues for DRS to operate. A warning message is displayed on the **Cluster Summary** page.

If DRS is non-functional this does not mean that DRS is deactivated. Existing DRS settings and resource pools survive across a lost vCLS VMs quorum. vCLS health turns **Unhealthy** only in a DRS activated cluster when vCLS VMs are not running and the first instance of DRS is skipped because of this. vCLS health will stay **Degraded** on a non-DRS activated cluster when at least one vCLS VM is not running.

Datastore selection for vCLS VMs

The datastore for vCLS VMs is automatically selected based on ranking all the datastores connected to the hosts inside the cluster. A datastore is more likely to be selected if there are hosts in the cluster with free reserved DRS slots connected to the datastore. The algorithm tries to place vCLS VMs in a shared datastore if possible before selecting a local datastore. A datastore with more free space is preferred and the algorithm tries not to place more than one vCLS VM on the same datastore. You can only change the datastore of vCLS VMs after they are deployed and powered on.

If you want to move the VMDKs for vCLS VMs to a different datastore or attach a different storage policy, you can reconfigure vCLS VMs. A warning message is displayed when you perform this operation.

You can perform a storage vMotion to migrate vCLS VMs to a different datastore. You can tag vCLS VMs or attach custom attributes if you want to group them separately from workload VMs, for instance if you have a specific meta-data strategy for all VMs that run in a data center.

Note: When a datastore is placed in maintenance mode, if the datastore hosts vCLS VMs, you must manually apply storage vMotion to the vCLS VMs to move them to a new location or put the cluster in retreat mode. A warning message is displayed.

```
The enter maintenance mode task will start but cannot finish because there is 1 virtual
 machine residing on the datastore. You can always cancel the task in your Recent Tasks if
 you decide to continue.
```

```
The selected datastore might be storing vSphere Cluster Services VMs which cannot be
 powered off. To ensure the health of vSphere Cluster Services, these VMs have to be
 manually vMotioned to a different datastore within the cluster prior to taking this
 datastore down for maintenance. Refer to this KB article: KB 79892.
```

Select the check box `Let me migrate storage for all virtual machines and continue entering maintenance mode after migration.` to proceed.

vCLS Datastore Placement

You can override default vCLS VM datastore placement.

vSphere Cluster Services (vCLS) VM datastore location is chosen by a default datastore selection logic. To override the default vCLS VM datastore placement for a cluster, you can specify a set of allowed datastores by browsing to the cluster and clicking **ADD** under **Configure** > **vSphere Cluster Service** > **Datastores**. Some datastores cannot be selected for vCLS because they are blocked by solutions like SRM or vSAN maintenance mode where vCLS cannot be configured. Users cannot add or remove Solution blocked datastores for vCLS VMs.

Monitoring vSphere Cluster Services

You can monitor the resources consumed by vCLS VMs and their health status.

vCLS VMs are not displayed in the inventory tree in the **Hosts and Clusters** tab. vCLS VMs from all clusters within a data center are placed inside a separate VMs and templates folder named **vCLS**. This folder and the vCLS VMs are visible only in the **VMs and Templates** tab of the vSphere Client. These VMs are identified by a different icon than regular workload VMs. You can view information about the purpose of the vCLS VMs in the **Summary** tab of the vCLS VMs.

You can monitor the resources consumed by vCLS VMs in the **Monitor** tab.

Table 334: vCLS VM Resource Allocation

Property	Size
VMDK size	245 MB (thin disk)
Memory	128 MB
CPU	1 vCPU
Hard disk	2 GB
Storage on datastore	480 MB (thin disk)

Note: Each vCLS VM has 100MHz and 100MB capacity reserved in the cluster. Depending on the number of vCLS VMs running in the cluster, a max of 400 MHz and 400 MB of capacity can be reserved for these VMs.

You can monitor the health status of vCLS in the **Cluster Services** portlet displayed in the **Summary** tab of the cluster.

Table 335: Health status of vCLS

Status	Color Coding	Summary
Healthy	Green	If there is at least one vCLS VM running, the status remains healthy, regardless of the number of hosts in the cluster.

Status	Color Coding	Summary
Degraded	Yellow	If there is no vCLS VM running for less than 3 minutes (180 seconds), the status is degraded.
Unhealthy	Red	If there is no vCLS VM running for 3 minutes or more, the status is unhealthy in a DRS enabled cluster.

Maintaining Health of vSphere Cluster Services

vCLS VMs are always powered-on because vSphere DRS depends on the availability of these VMs. These VMs should be treated as system VMs. Only administrators can perform selective operations on vCLS VMs. To avoid failure of cluster services, avoid performing any configuration or operations on the vCLS VMs.

vCLS VMs are protected from accidental deletion. Cluster VMs and folders are protected from modification by users, including administrators.

Only users which are part of the Administrators SSO group can perform the following operations::

- ReadOnly access for vCLS VMs
- Console access to vCLS VMs
- Relocate vCLS VMs to either new storage, compute resource or both using cold or hot migration
- Power off vCLS VMs

Operations that might disrupt the healthy functioning of vCLS VMs:

- Changing the power state of the vCLS VMs
- Resource reconfiguration of the vCLS VMs such as changing CPU, Memory, Disk size, Disk placement
- VM encryption
- Triggering vMotion of the vCLS VMs
- Changing the BIOS
- Removing the vCLS VMs from the inventory
- Deleting the vCLS VMs from disk
- Enabling FT of vCLS VMs
- Cloning vCLS VMs
- Configuring PMem
- Moving vCLS VM to a different folder
- Renaming the vCLS VMs
- Renaming the vCLS folders
- Enabling DRS rules and overrides on vCLS VMs
- Enabling HA admission control policy on vCLS VMs
- Enabling HA overrides on vCLS VMs
- Moving vCLS VMs to a resource pool
- Recovering vCLS VMs from a snapshot

When you perform any disruptive operation on the vCLS VMs, a warning dialog box appears.

Troubleshooting:

The health of vCLS VMs, including power state, is managed by EAM and WCP services. In case of power on failure of vCLS VMs, or if the first instance of DRS for a cluster is skipped due to lack of quorum of vCLS VMs, a banner appears in the cluster summary page along with a link to a Knowledge Base article to help troubleshoot the error state.

Because vCLS VMs are treated as system VMs, you do not need to backup or snapshot these VMs. The health state of these VMs is managed by vCenter services.

Putting a Cluster in Retreat Mode

When a datastore is placed in maintenance mode, if the datastore hosts vCLS VMs, you must manually storage vMotion the vCLS VMs to a new location or put the cluster in retreat mode.

This task explains how to put a cluster in retreat mode.

1. Login to the vSphere Client.
2. Navigate to the cluster on which vCLS must be deactivated.
3. Copy the cluster domain ID from the URL of the browser. It should be similar to `domain-c(number)`.

   Note: Only copy the numbers to the left of the colon in the URL.
4. Navigate to the vCenter Server **Configure** tab.
5. Under **Advanced Settings**, click the **Edit Settings** button.
6. Add a new entry `config.vcls.clusters.domain-c(number).enabled`. Use the domain ID copied in step 3.
7. Set the **Value** to `False`.
8. Click **Save**.

vCLS monitoring service runs every 30 seconds. Within 1 minute, all the vCLS VMs in the cluster are cleaned up and the **Cluster Services** health will be set to **Degraded**. If the cluster has DRS activated, it stops functioning and an additional warning is displayed in the **Cluster Summary**. DRS is not functional, even if it is activated, until vCLS is reconfigured by removing it from Retreat Mode.

vSphere HA does not perform optimal placement during a host failure scenario. HA depends on DRS for placement recommendations. HA will still power on the VMs but these VMs might be powered on in a less optimal host.

To remove Retreat Mode from the cluster, change the value in step 7 to `True`.

Retrieving Password for vCLS VMs

You can retrieve the password to login to the vCLS VMs.

To ensure cluster services health, avoid accessing the vCLS VMs. This document is intended for explicit diagnostics on vCLS VMs.

1. Use SSH to login to the vCenter Server Appliance.
2. Run the following python script:
   `/usr/lib/vmware-wcp/decrypt_clustervm_pw.py`
3. Read the output for the password.

   pwd-script-output

   ```
   Read key from file
   Connected to PSQL
   PWD: (password displayed here)
   ```

With the retrieved password, you can log into the vCLS VMs.

vCLS VM Anti-Affinity Policies

vSphere supports anti-affinity between vCLS VMs and another group of workload VMs.

Compute policies provide a way to specify how the vSphere Distributed Resource Scheduler (DRS) should place VMs on hosts in a resource pool. Use the vSphere Compute Policies editor to create and delete compute policies. You can create or delete, but not modify, a compute policy. If you delete a category tag used in the definition of the policy, the policy is also deleted. Open the **VM Summary** page in vSphere to view the compute policies that apply to a VM and its compliance status with each policy. You can create a compute policy for a group of workload VMs that is anti-affine to the group of vCLS VMs. A vCLS anti-affinity policy can have a single user visible tag for a group of workload VMs, and the other group of vCLS VMs is internally recognized.

Create or Delete a vCLS VM Anti-Affinity Policy

A vCLS VM anti-affinity policy describes a relationship between a category of VMs and vCLS system VMs.

A vCLS VM anti-affinity policy discourages placement of vCLS VMs and application VMs on the same host. This kind of policy can be useful when you do not want vCLS VMs and virtual machines running critical workload to run on the same host. Some best practices for running critical workloads such as SAP HANA require dedicated hosts. After the policy is created, the placement engine attempts to place vCLS VMs on the hosts where policy VMs are not running.

Enforcement of a vCLS VM anti-affinity policy can be affected in several ways:

- If the policy applies to multiple VMs on different hosts and it is not possible to have enough hosts to distribute vCLS VMs, vCLS VMs are consolidated into the hosts without policy VMs.
- If a provisioning operation specifies a destination host, that specification is always honored even if it violates the policy. DRS will try to move the vCLS VMs to a compliant host in a subsequent remediation cycle.

1. Create a category and tag for each group of VMs that you want to include in a vCLS VM anti-affinity policy.
2. Tag the VMs that you want to include.
3. Create a vCLS VM anti-affinity policy.
   a) From the vSphere, click **Policies and Profiles** > **Compute Policies**.
   b) Click **Add** to open the **New Compute Policy** Wizard.
   c) Fill in the policy **Name** and choose **vCLS VM anti affinity** from the **Policy type** drop-down control.
      The policy **Name** must be unique.
   d) Provide a **Description** of the policy, then use **VM tag** to choose the **Category** and **Tag** to which the policy applies.
      Unless you have multiple VM tags associated with a category, the wizard fills in the VM tag after you select the tag **Category**.
   e) Click **Create** to create the policy.
4. Optional: To delete a compute policy, open vSphere, click **Policies and Profiles** > **Compute Policies** to show each policy as a card. Click DELETE to delete a policy.

Admission Control and Initial Placement

When you attempt to power on a single virtual machine or a group of virtual machines in a DRS-enabled cluster, vCenter Server performs admission control. It checks that there are enough resources in the cluster to support the virtual machine(s).

If the cluster does not have sufficient resources to power on a single virtual machine, or any of the virtual machines in a group power-on attempt, a message appears. Otherwise, for each virtual machine, DRS generates a recommendation of a host on which to run the virtual machine and takes one of the following actions

- Automatically executes the placement recommendation.

- Displays the placement recommendation, which the user can then choose to accept or override.
  Note: No initial placement recommendations are given for virtual machines on standalone hosts or in non-DRS clusters. When powered on, they are placed on the host where they currently reside.
- DRS considers network bandwidth. By calculating host network saturation, DRS is able to make better placement decisions. This can help avoid performance degradation of virtual machines with a more comprehensive understanding of the environment.

Single Virtual Machine Power On

In a DRS cluster, you can power on a single virtual machine and receive initial placement recommendations.

When you power on a single virtual machine, you have two types of initial placement recommendations:

- A single virtual machine is being powered on and no prerequisite steps are needed.
  The user is presented with a list of mutually exclusive initial placement recommendations for the virtual machine. You can select only one.
- A single virtual machine is being powered on, but prerequisite actions are required.
  These actions include powering on a host in standby mode or the migration of other virtual machines from one host to another. In this case, the recommendations provided have multiple lines, showing each of the prerequisite actions. The user can either accept this entire recommendation or cancel powering on the virtual machine.

Group Power-on

You can attempt to power on multiple virtual machines at the same time (group power-on).

Virtual machines selected for a group power-on attempt do not have to be in the same DRS cluster. They can be selected across clusters but must be within the same data center. It is also possible to include virtual machines located in non-DRS clusters or on standalone hosts. These virtual machines are powered on automatically and not included in any initial placement recommendation.

The initial placement recommendations for group power-on attempts are provided on a per-cluster basis. If all the placement-related actions for a group power-on attempt are in automatic mode, the virtual machines are powered on with no initial placement recommendation given. If placement-related actions for any of the virtual machines are in manual mode, the powering on of all the virtual machines (including the virtual machines that are in automatic mode) is manual. These actions are included in an initial placement recommendation.

For each DRS cluster that the virtual machines being powered on belong to, there is a single recommendation, which contains all the prerequisites (or no recommendation). All such cluster-specific recommendations are presented together under the **Power On Recommendations** tab.

When a nonautomatic group power-on attempt is made, and virtual machines not subject to an initial placement recommendation (that is, the virtual machines on standalone hosts or in non-DRS clusters) are included, vCenter Server attempts to power them on automatically. If these power-ons are successful, they are listed under the **Started Power-Ons** tab. Any virtual machines that fail to power-on are listed under the **Failed Power-Ons** tab.

Group Power-on

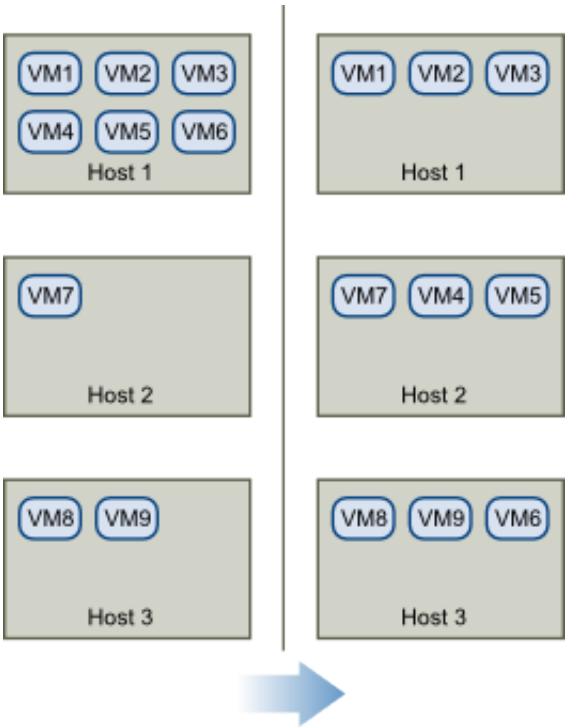
The user selects three virtual machines in the same data center for a group power-on attempt. The first two virtual machines (VM1 and VM2) are in the same DRS cluster (Cluster1), while the third virtual machine (VM3) is on a standalone host. VM1 is in automatic mode and VM2 is in manual mode. For this scenario, the user is presented with an initial placement recommendation for Cluster1 (under the **Power On Recommendations** tab) which consists of actions for powering on VM1 and VM2. An attempt is made to power on VM3 automatically and, if successful, it is listed under the **Started Power-Ons** tab. If this attempt fails, it is listed under the **Failed Power-Ons** tab.

Virtual Machine Migration

Although DRS performs initial placements so that load is balanced across the cluster, changes in virtual machine load and resource availability can cause the cluster to become unbalanced. To correct such imbalances, DRS generates migration recommendations.

If DRS is enabled on the cluster, load can be distributed more uniformly to reduce the degree of this imbalance. For example, the three hosts on the left side of the following figure are unbalanced. Assume that Host 1, Host 2, and Host 3 have identical capacity, and all virtual machines have the same configuration and load (which includes reservation, if set). However, because Host 1 has six virtual machines, its resources might be overused while ample resources are available on Host 2 and Host 3. DRS migrates (or recommends the migration of) virtual machines from Host 1 to Host 2 and Host 3. On the right side of the diagram, the properly load balanced configuration of the hosts that results appears.

Figure 104: Load Balancing



When a cluster becomes unbalanced, DRS makes recommendations or migrates virtual machines, depending on the default automation level:

- If the cluster or any of the virtual machines involved are manual or partially automated, vCenter Server does not take automatic actions to balance resources. Instead, the Summary page indicates that migration recommendations are available and the DRS Recommendations page displays recommendations for changes that make the most efficient use of resources across the cluster.
- If the cluster and virtual machines involved are all fully automated, vCenter Server migrates running virtual machines between hosts as needed to ensure efficient use of cluster resources.

  Note: Even in an automatic migration setup, users can explicitly migrate individual virtual machines, but vCenter Server might move those virtual machines to other hosts to optimize cluster resources.

By default, automation level is specified for the whole cluster. You can also specify a custom automation level for individual virtual machines.

DRS Migration Threshold

The DRS migration threshold allows you to specify which recommendations are generated and then applied (when the virtual machines involved in the recommendation are in fully automated mode) or shown (if in manual mode). This threshold is a measure of how aggressive DRS is in recommending migrations to improve VM happiness.

You can move the threshold slider to use one of five settings, ranging from Conservative to Aggressive. The higher the agressiveness setting, the more frequently DRS might recommend migrations to improve VM happiness. The Conservative setting generates only priority-one recommendations (mandatory recommendations).

After a recommendation receives a priority level, this level is compared to the migration threshold you set. If the priority level is less than or equal to the threshold setting, the recommendation is either applied (if the relevant virtual machines are in fully automated mode) or displayed to the user for confirmation (if in manual or partially automated mode.)

DRS Score

Each migration recommendation is computed using the VM happiness metric which measures execution efficiency. This metric is displayed as DRS Score in the cluster's Summary tab in the vSphere Client. DRS load balancing recommendations attempt to improve the DRS score of a VM. The Cluster DRS score is a weighted average of the VM DRS Scores of all the powered on VMs in the cluster. The Cluster DRS Score is shown in the gauge component. The color of the filled in section changes depending on the value to match the corresponding bar in the VM DRS Score histogram. The bars in the histogram show the percentage of VMs that have a DRS Score in that range. You can view the list with server-side sorting and filtering by selecting the Monitor tab of the cluster and selecting vSphere DRS, which shows a list of the VMs in the cluster sorted by their DRS score in ascending order.

Migration Recommendations

If you create a cluster with a default manual or partially automated mode, vCenter Server displays migration recommendations on the DRS Recommendations page.

The system supplies as many recommendations as necessary to enforce rules and balance the resources of the cluster. Each recommendation includes the virtual machine to be moved, current (source) host and destination host, and a reason for the recommendation. The reason can be one of the following:

- Balance average CPU loads or reservations.
- Balance average memory loads or reservations.
- Satisfy resource pool reservations.
- Satisfy an affinity rule.
- Host is entering maintenance mode or standby mode.

Note: If you are using the vSphere Distributed Power Management (DPM) feature, in addition to migration recommendations, DRS provides host power state recommendations.

DRS Cluster Requirements

Hosts that are added to a DRS cluster must meet certain requirements to use cluster features successfully.

Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services for more information.

Shared Storage Requirements

A DRS cluster has certain shared storage requirements.

Ensure that the managed hosts use shared storage. Shared storage is typically on a SAN, but can also be implemented using NAS shared storage.

See the *vSphere Storage* documentation for information about other shared storage.

Shared VMFS Volume Requirements

A DRS cluster has certain shared VMFS volume requirements.

Configure all managed hosts to use shared VMFS volumes.

- Place the disks of all virtual machines on VMFS volumes that are accessible by source and destination hosts.
- Ensure the VMFS volume is sufficiently large to store all virtual disks for your virtual machines.
- Ensure all VMFS volumes on source and destination hosts use volume names, and all virtual machines use those volume names for specifying the virtual disks.

Note: Virtual machine swap files also need to be on a VMFS accessible to source and destination hosts (just like `.vmdk` virtual disk files). This requirement does not apply if all source and destination hosts are ESX Server 3.5 or higher and using host-local swap. In that case, vMotion with swap files on unshared storage is supported. Swap files are placed on a VMFS by default, but administrators might override the file location using advanced virtual machine configuration options.

Processor Compatibility Requirements

A DRS cluster has certain processor compatibility requirements.

To avoid limiting the capabilities of DRS, you should maximize the processor compatibility of source and destination hosts in the cluster.

vMotion transfers the running architectural state of a virtual machine between underlying ESXi hosts. vMotion compatibility means that the processors of the destination host must be able to resume execution using the equivalent instructions where the processors of the source host were suspended. Processor clock speeds and cache sizes might vary, but processors must come from the same vendor class (Intel versus AMD) and the same processor family to be compatible for migration with vMotion.

Processor families are defined by the processor vendors. You can distinguish different processor versions within the same family by comparing the processors' model, stepping level, and extended features.

Sometimes, processor vendors have introduced significant architectural changes within the same processor family (such as 64-bit extensions and SSE3). VMware identifies these exceptions if it cannot guarantee successful migration with vMotion.

vCenter Server provides features that help ensure that virtual machines migrated with vMotion meet processor compatibility requirements. These features include:

- Enhanced vMotion Compatibility (EVC) – You can use EVC to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.
  Configure EVC from the Cluster Settings dialog box. The hosts in a cluster must meet certain requirements for the cluster to use EVC. For information about EVC and EVC requirements, see the *vCenter Server and Host Management* documentation.
- CPU compatibility masks – vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migrations with vMotion. By applying CPU compatibility masks to individual virtual machines, you can hide certain CPU features from the virtual machine and potentially prevent migrations with vMotion from failing due to incompatible CPUs.

vMotion Requirements for DRS Clusters

A DRS cluster has certain vMotion requirements.

To enable the use of DRS migration recommendations, the hosts in your cluster must be part of a vMotion network. If the hosts are not in the vMotion network, DRS can still make initial placement recommendations.

To be configured for vMotion, each host in the cluster must meet the following requirements:

- vMotion does not support raw disks or migration of applications clustered using Microsoft Cluster Service (MSCS).
- vMotion requires a private Gigabit Ethernet migration network between all of the vMotion enabled managed hosts. When vMotion is enabled on a managed host, configure a unique network identity object for the managed host and connect it to the private migration network.

Configuring DRS with Virtual Flash

DRS can manage virtual machines that have virtual flash reservations.

Virtual flash capacity appears as a statistic that is regularly reported from the host to the vSphere Client. Each time DRS runs, it uses the most recent capacity value reported.

You can configure one virtual flash resource per host. This means that during virtual machine power-on time, DRS does not need to select between different virtual flash resources on a given host.

DRS selects a host that has sufficient available virtual flash capacity to start the virtual machine. If DRS cannot satisfy the virtual flash reservation of a virtual machine, it cannot be powered-on. DRS treats a powered-on virtual machine with a virtual flash reservation as having a soft affinity with its current host. DRS will not recommend such a virtual machine for vMotion except for mandatory reasons, such as putting a host in maintenance mode, or to reduce the load on an over utilized host.

Create a Cluster

A cluster is a group of hosts. When a host is added to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts within it.

- Verify that you have sufficient permissions to create a cluster object.
- Verify that a data center exists in the inventory.
- If you want to use vSAN, it must be enabled before you configure vSphere HA.

Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.
Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services for more information.

1. Browse to a data center in the vSphere Client.
2. Right-click the data center and select **New Cluster**.
3. Enter a name for the cluster.
4. Select DRS and vSphere HA cluster features.

Option	Description
To use DRS with this cluster	1. Select the DRS **Turn ON** check box. 2. Select an automation level and a migration threshold.
To use HA with this cluster	1. Select the vSphere HA **Turn ON** check box. 2. Select whether to enable host monitoring and admission control. 3. If admission control is enabled, specify a policy.

Option	Description
	4. Select a VM Monitoring option. 5. Specify the virtual machine monitoring sensitivity.

5. Select an Enhanced vMotion Compatibility (EVC) setting.

   EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.

6. Click **OK**.

The cluster is added to the inventory.

Add hosts and resource pools to the cluster.

Note: Under the **Cluster Summary** page, you can see **Cluster Services** which displays vSphere Cluster Services health status.

Edit Cluster Settings

When you add a host to a DRS cluster, the host's resources become part of the cluster's resources. In addition to this aggregation of resources, with a DRS cluster you can support cluster-wide resource pools and enforce cluster-level resource allocation policies.

You can create a cluster without a special license, but you must have a license to enable a cluster for vSphere DRS or vSphere HA.

Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services for more information.

The following cluster-level resource management capabilities are also available.

Load Balancing	The distribution and usage of CPU and memory resources for all hosts and virtual machines in the cluster are continuously monitored. DRS compares these metrics to an ideal resource usage given the attributes of the cluster's resource pools and virtual machines, the current demand, and the imbalance target. DRS then provides recommendations or performs virtual machine migrations accordingly. See Virtual Machine Migration. When you power on a virtual machine in the cluster, DRS attempts to maintain proper load balancing by either placing the virtual machine on an appropriate host or making a recommendation. See Admission Control and Initial Placement.
Power management	When the vSphere Distributed Power Management (DPM) feature is enabled, DRS compares cluster and host-level capacity to the demands of the cluster's virtual machines, including recent historical demand. DRS then recommends you place hosts in standby, or places hosts in standby power mode when sufficient excess capacity is found. DRS powers-on hosts if capacity is needed. Depending on the resulting host power state recommendations, virtual machines might need to be migrated to and from the hosts as well. See Managing Power Resources.

Affinity Rules

You can control the placement of virtual machines on hosts within a cluster, by assigning affinity rules. See Using Affinity Rules with vSphere DRS.

1. Browse to a cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Under **vSphere DRS** click **Edit**.
4. Under **DRS Automation**, select a default automation level for DRS.

Automation Level	Action
Manual	• Initial placement: Recommended host is displayed. • Migration: Recommendation is displayed.
Partially Automated	• Initial placement: Automatic. • Migration: Recommendation is displayed.
Fully Automated	• Initial placement: Automatic. • Migration: Recommendation is run automatically.

5. Set the **Migration Threshold** for DRS.
6. Select the **Predictive DRS** check box. In addition to real-time metrics, DRS responds to forecasted metrics provided by vRealize Operations server. You must also configure **Predictive DRS** in a version of vRealize Operations that supports this feature.
7. Select **Virtual Machine Automation** check box to enable individual virtual machine automation levels.

   Override for individual virtual machines can be set from the VM Overrides page.
8. Under **Additional Options**, select a check box to enforce one of the default policies.

Option	Description
VM Distribution	For availability, distribute a more even number of virtual machines across hosts. This is secondary to DRS load balancing.
Memory Metric for Load Balancing	Load balance based on consumed memory of virtual machines rather than active memory. This setting is only recommended for clusters where host memory is not over-committed. **Note:** This setting is no longer supported and will not be displayed in vCenter 7.0.
CPU Over-Commitment	Control CPU over-commitment in the cluster.
Scalable Shares	Enable scalable shares for the resource pools on this cluster.

9. Under **Power Management**, select Automation Level.
10. If DPM is enabled, set the **DPM Threshold**.
11. Click **OK**.

Note: Under the **Cluster Summary** page, you can see **Cluster Services** which displays vSphere Cluster Services health status.

You can view memory utilization for DRS in the vSphere Client. To find out more, see: Viewing Distributed Resource Scheduler Memory Utilization

Set a Custom Automation Level for a Virtual Machine

After you create a DRS cluster, you can customize the automation level for individual virtual machines to override the cluster's default automation level.

For example, you can select **Manual** for specific virtual machines in a cluster with full automation, or **Partially Automated** for specific virtual machines in a manual cluster.

If a virtual machine is set to **Disabled**, vCenter Server does not migrate that virtual machine or provide migration recommendations for it.

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Under Services, select **vSphere DRS** and click **Edit**. Expand DRS Automation.
4. Select the **Enable individual virtual machine automation levels** check box.
5. To temporarily deactivate any individual virtual machine overrides, deselect the **Enable individual virtual machine automation levels** check box.

   Virtual machine settings are restored when the check box is selected again.
6. To temporarily suspend all vMotion activity in a cluster, put the cluster in manual mode and deselect the **Enable individual virtual machine automation levels** check box.
7. Select one or more virtual machines.
8. Click the **Automation Level** column and select an automation level from the drop-down menu.

Option	Description
Manual	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.
Partially Automated	Initial placement is performed automatically. Migration recommendations are displayed, but do not run.
Disabled	vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

9. Click **OK**.

Note:

Other VMware products or features, such as vSphere vApp and vSphere Fault Tolerance, might override the automation levels of virtual machines in a DRS cluster. Refer to the product-specific documentation for details.

Deactivate DRS

You can turn off DRS for a cluster.

When DRS is deactivated:

- DRS affinity rules are not removed but are not applied until DRS is reactivated.
- Host and VM groups are not removed but are not applied until DRS is reactivated.
- Resource pools are permanently removed from the cluster. To avoid losing the resource pools, save a snapshot of the resource pool tree on your local machine. You can use the snapshot to restore the resource pool when you activate DRS.

Note: Do not deactivate DRS if Workload Management is activated, this makes WCP services unrecoverable.

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Under **vSphere DRS**, click **Edit**.
4. Deselect the **Turn On vSphere DRS** check box.
5. Click **OK** to turn off DRS.
6. Optional: Choose an option to save the resource pool.
   - Click **Yes** to save a resource pool tree snapshot on a local machine.
   - Click **No** to turn off DRS without saving a resource pool tree snapshot.

DRS is turned off.
Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services for more information.

Restore a Resource Pool Tree

You can restore a previously saved resource pool tree snapshot.

- vSphere DRS must be turned ON.
- You can restore a snapshot only on the same cluster that it was taken.
- No other resource pools are present in the cluster.
- Backup and restore must always be performed on the same version of vCenter and ESXi.

1. Browse to the cluster in the vSphere Client.
2. Select the cluster and click the **Configure** tab.
3. Under **Services**, click **vSphere DRS**.
4. Click **Restore Resource Pool Tree**.
5. Click **Browse**, and locate the snapshot file on your local machine.
6. Click **Open**.
7. Click **OK** to restore the resource pool tree.

DRS Awareness of vSAN Stretched Cluster

DRS Awareness of vSAN Stretched Cluster is available on stretched clusters with DRS enabled using vSphere 7.0 U2. A vSAN stretched cluster has read locality, where the VM reads data from a local site. Fetching reads from a remote site can affect VM performance. In releases prior to vSphere 7.0 U2, DRS had no awareness of read locality for a vSAN stretched clusters and might inadvertently place a VM on a remote site with no read locality. With DRS Awareness of vSAN Stretched Cluster, DRS is now fully aware of VM read locality and will place the VM on a site that can fully satisfy the read locality. This is automatic, there are no configurable options. DRS Awareness of vSAN Stretched Cluster works with existing affinity rules. It works with vSphere 7.0 U2 and VMware Cloud on AWS.

vSAN Stretched Cluster with vSphere HA and vSphere DRS provide resiliency by having two copies of data spread across two fault domains and a witness node in a third fault domain in case of failures. The two active fault domains provide replication of data so that both fault domains have a current copy of the data.

vSAN Stretched Cluster provides an automated method of moving workloads within the two fault domains. In case of full site failures, VMs are restarted on the secondary site by vSphere HA. This ensures that there is no downtime for critical production workloads. Once the primary site is back online, DRS immediately rebalances the VMs back to the primary

site with soft affinity hosts. This process causes the VM to read and write from the secondary site while the VM data components are still rebuilding and might reduce VM performance.

In releases prior to vSphere 7.0 U2, we recommend that you change DRS from fully automated to partially automated mode, to avoid VMs migrating while resynchronization is in progress to the primary site. Set DRS back to fully automated only after the resynchronization is complete.

With vSphere 7.0 U2, DRS Awareness of vSAN Stretched Cluster introduces a fully automated read locality solution for recovering from failures on a vSAN stretched cluster. The read locality information indicates the hosts the VM has full access to, and DRS uses this information when placing a VM on a host on vSAN Stretched Clusters. DRS prevents VMs from failing back to the primary site when vSAN resynchronization is still in progress during the site recovery phase. DRS automatically migrates a VM back to the primary affined site when its data components have achieved full read locality. This allows you to operate DRS in fully automatic mode in case of full site failures.

In case of partial site failures, if a VM loses read locality due to loss of data components greater than or equal to its Failures to Tolerate vSphere DRS will identify the VMs that consume a very high read bandwidth and try to rebalance them to the secondary site. This ensures that VMs with read-heavy workloads do not decrease during partial site failures. Once the primary site is back online and the data components have completed resynchronization, the VM is moved back to the site it is affined to.

DRS Maintenance Mode Functionality with ROBO Enterprise License

In vSphere 6.7 U2, VMware's large Remote Office Branch Office (ROBO) Enterprise license supports automatic VM evacuations when a host enters maintenance mode.

In a ROBO Enterprise cluster, DRS is deactivated by default and you cannot make changes to DRS configuration. When a host in a ROBO Enterprise cluster enters maintenance mode, VMs are automatically evacuated from the host by DRS. Before evacuating the VMs from the host, DRS creates VM-host affinity mappings to track where the VMs were placed. When the host exits maintenance mode, the VMs that were running on the host are migrated back to the host. VM-host affinity mappings are cleared after the migration.

Limitations of DRS Maintenance Mode with ROBO Enterprise License

DRS Functionality with ROBO Enterprise License is not full DRS functionality.

There are some limitations you should be aware of before you initiate maintenance mode on a ROBO Enterprise cluster. On a ROBO Enterprise cluster, DRS is deactivated by default. If you have migrated from a DRS supported license to a ROBO Enterprise license, you may have VMs with affinity or anti-affinity rules present in the system. You must deactivate or delete VMs with affinity or anti-affinity rules or the ROBO Enterprise maintenance mode operation is deactivated. ROBO Enterprise maintenance mode operation is deactivated if DRS is not set to fully automated mode. DRS automation level must be set to fully automated mode in order to evacuate VMs automatically through the host maintenance workflow. If a VM overrides DRS fully automated mode, you must evacuate the VM manually.

Note: `ClusterEnterMaintenanceMode` is an API that takes a list of hosts in the cluster as input and returns a recommendation of hosts that the server can successfully evacuate given the existing constraints in the cluster. This API is not available with the ROBO Enterprise license.

Note: Due to dependency on ClusterEnterMaintenanceMode API, VMware vLCM cannot automatically put hosts into Maintenance Mode during full cluster remediation if there are VMs on the hosts.

Using DRS Maintenance Mode with ROBO Enterprise License

vSphere 6.7 U2 supports limited DRS Maintenance Mode functionality with ROBO Enterprise License.

- Check if all hosts in a cluster have the ROBO Enterprise License installed. If they do not, you must install the license.

- Check whether any DRS rules are configured and activated. If they are, you must deactivate or delete them to use ROBO Enterprise maintenance mode operation.

1. In order for DRS Maintenance Mode to work with ROBO Enterprise License, make sure that each host on the cluster has the ROBO Enterprise License installed.
   - If the license is not installed, go to step 2.
   - If the license is installed, go to step 3.
2. Install the ROBO Enterprise License
   a) Browse to the host in the vSphere Client.
   b) Under the **Configure** tab, select **Licensing**.
   c) Click **ASSIGN LICENSE**.
   d) Enter your ROBO Enterprise License key and click **OK**.

   You must repeat these steps for all hosts in the cluster.
3. Select the host in the cluster, right-click and select **Enter Maintenance Mode** and click **OK**.

   The VMs on the host are automatically evacuated.

After the host exits Maintenance Mode, the VMs are automatically migrated back to the host. The host is restored to the original state. However, if a host is overloaded DRS cannot migrate VMs back to the original host. DRS attempts to restore the host to the original state, but it cannot make a host overloaded.

If you need to deactivate DRS Maintenance Mode with ROBO Enterprise License, you can edit the vpxd.cfg file. Open the vpxd.cfg file. Under the `<cluster>` option, change `<roboMMEnabled>true</roboMMEnabled>` to `<roboMMEnabled>false</roboMMEnabled>`. This is runtime configuration, so you do not need to restart vpxd after updating the configuration.

Troubleshooting DRS Maintenance Mode with ROBO Enterprise License

If you experience issues using maintenance mode with your ROBO Enterprise cluster, consider the following.

In order for maintenance mode to function correctly with a ROBO Enterprise cluster:

- Check if all hosts in a cluster have the ROBO Enterprise License installed. If they do not, you must install the license.
- Check whether any DRS rules are configured and activated. If they are, you must deactivate or delete them to use ROBO Enterprise maintenance mode operation.
- If the compatibility check fails, make sure that the other hosts are compatible with the VM.

Using DRS Clusters to Manage Resources

After you create a DRS cluster, you can customize it and use it to manage resources.

To customize your DRS cluster and the resources it contains you can configure affinity rules and you can add and remove hosts and virtual machines. When a cluster’s settings and resources have been defined, you should ensure that it is and remains a valid cluster. You can also use a valid DRS cluster to manage power resources and interoperate with vSphere HA.

Note: In this chapter, "Memory" can refer to physical RAM or Persistent Memory.

Adding Hosts to a Cluster

The procedure for adding hosts to a cluster is different for hosts managed by the same vCenter Server (managed hosts) than for hosts not managed by that server.

After a host has been added, the virtual machines deployed to the host become part of the cluster and DRS can recommend migration of some virtual machines to other hosts in the cluster.

Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services for more information.

Add a Managed Host to a Cluster

When you add a standalone host already being managed by vCenter Server to a DRS cluster, the host's resources become associated with the cluster.

You can decide whether you want to associate existing virtual machines and resource pools with the cluster's root resource pool or graft the resource pool hierarchy.

Note: If a host has no child resource pools or virtual machines, the host's resources are added to the cluster but no resource pool hierarchy with a top-level resource pool is created.

1. Browse to the host in the vSphere Client.
2. Right-click the host and select **Move To...**.
3. Select a cluster.
4. Click **OK** to apply the changes.
5. Select what to do with the host's virtual machines and resource pools.
   - **Put this host's virtual machines in the cluster's root resource pool**

     vCenter Server removes all existing resource pools of the host and the virtual machines in the host's hierarchy are all attached to the root. Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares after selecting this option, which destroys the resource pool hierarchy.
   - **Create a resource pool for this host's virtual machines and resource pools**

     vCenter Server creates a top-level resource pool that becomes a direct child of the cluster and adds all children of the host to that new resource pool. You can supply a name for that new top-level resource pool. The default is **Grafted from <host_name>**.

The host is added to the cluster.

Add an Unmanaged Host to a Cluster

You can add an unmanaged host to a cluster. Such a host is not currently managed by the same vCenter Server system as the cluster and it is not visible in the vSphere Client.

1. Browse to the cluster in the vSphere Client.
2. Right-click the cluster and select **Add Host**.
3. Enter the host name, user name, and password, and click **Next**.
4. View the summary information and click **Next**.
5. Assign an existing or a new license key and click **Next**.
6. Optional: You can enable lockdown mode to prevent remote users from logging directly into the host.

   If you do not enable lockdown mode, you can configure this option later by editing Security Profile in host settings.

7. Select what to do with the host's virtual machines and resource pools.
   - **Put this host's virtual machines in the cluster's root resource pool**

     vCenter Server removes all existing resource pools of the host and the virtual machines in the host's hierarchy are all attached to the root. Because share allocations are relative to a resource pool, you might have to manually change a virtual machine's shares after selecting this option, which destroys the resource pool hierarchy.
   - **Create a resource pool for this host's virtual machines and resource pools**

     vCenter Server creates a top-level resource pool that becomes a direct child of the cluster and adds all children of the host to that new resource pool. You can supply a name for that new top-level resource pool. The default is **Grafted from <host_name>**.
8. Review settings and click **Finish**.

The host is added to the cluster.

Adding Virtual Machines to a Cluster

You can add a virtual machine to a cluster in a number of ways.

- When you add a host to a cluster, all virtual machines on that host are added to the cluster.
- When a virtual machine is created, the **New Virtual Machine** wizard prompts you for the location to place the virtual machine. You can select a standalone host or a cluster and you can select any resource pool inside the host or cluster.
- You can migrate a virtual machine from a standalone host to a cluster or from a cluster to another cluster using the **Migrate Virtual Machine** wizard. To start this wizard, right-click the virtual machine name and select **Migrate**.

Move a Virtual Machine to a Cluster

You can move a virtual machine to a cluster.

1. Find the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click on the virtual machine and select **Move To...**.
3. Select a cluster.
4. Click **OK**.

Removing Virtual Machines from a Cluster

You can remove virtual machines from a cluster.

You can remove a virtual machine from a cluster in two ways.

- When you remove a host from a cluster, all of the powered-off virtual machines that you do not migrate to other hosts are removed as well. You can remove a host only if it is in maintenance mode or disconnected. If you remove a host from a DRS cluster, the cluster can become yellow because it is overcommitted.
- You can migrate a virtual machine from a cluster to a standalone host or from a cluster to another cluster using the **Migrate** wizard. To start this wizard right-click the virtual machine name and select **Migrate**.

Move a Virtual Machine Out of a Cluster

You can move a virtual machine out of a cluster.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and select **Migrate**.
3. Select **Change datastore** and click **Next**.
4. Select a datastore and click **Next**.
5. Click **Finish**.

   If the virtual machine is a member of a DRS cluster rules group, vCenter Server displays a warning before it allows the migration to proceed. The warning indicates that dependent virtual machines are not migrated automatically. You have to acknowledge the warning before migration can proceed.

Removing a Host from a Cluster

When you remove a host from a DRS cluster, you affect resource pool hierarchies, virtual machines, and you might create invalid clusters. Consider the affected objects before you remove the host.

- Resource Pool Hierarchies – When you remove a host from a cluster, the host retains only the root resource pool, even if you used a DRS cluster and decided to graft the host resource pool when you added the host to the cluster. In that case, the hierarchy remains with the cluster. You can create a host-specific resource pool hierarchy.

  Note: Ensure that you remove the host from the cluster by first placing it in maintenance mode. If you instead disconnect the host before removing it from the cluster, the host retains the resource pool that reflects the cluster hierarchy.
- Virtual Machines – A host must be in maintenance mode before you can remove it from the cluster and for a host to enter maintenance mode all powered-on virtual machines must be migrated off that host. When you request that a host enter maintenance mode, you are also asked whether you want to migrate all the powered-off virtual machines on that host to other hosts in the cluster.
- Invalid Clusters – When you remove a host from a cluster, the resources available for the cluster decrease. If the cluster has enough resources to satisfy the reservations of all virtual machines and resource pools in the cluster, the cluster adjusts resource allocation to reflect the reduced amount of resources. If the cluster does not have enough resources to satisfy the reservations of all resource pools, but there are enough resources to satisfy the reservations for all virtual machines, an alarm is issued and the cluster is marked yellow. DRS continues to run.

Place a Host in Maintenance Mode

You place a host in maintenance mode when you need to service it, for example, to install more memory. A host enters or leaves maintenance mode only as the result of a user request.

Virtual machines that are running on a host entering maintenance mode need to be migrated to another host (either manually or automatically by DRS) or shut down. The host is in a state of **Entering Maintenance Mode** until all running virtual machines are powered down or migrated to different hosts. You cannot power on virtual machines or migrate virtual machines to a host entering maintenance mode.

When no more running virtual machines are on the host, the host's icon changes to include **under maintenance** and the host's Summary panel indicates the new state. While in maintenance mode, the host does not allow you to deploy or power on a virtual machine.

Note: DRS does not recommend (or perform, in fully automated mode) any virtual machine migrations off of a host entering maintenance or standby mode if the vSphere HA failover level would be violated after the host enters the requested mode.

1. Browse to the host in the vSphere Client.
2. Right-click the host and select **Maintenance Mode** > **Enter Maintenance Mode**.
   - If the host is part of a partially automated or manual DRS cluster, browse to **Cluster** > **Monitor** > **DRS** > **Recommendations** and click **Apply Recommendations**.
   - If the host is part of an automated DRS cluster, virtual machines are migrated to different hosts when the host enters maintenance mode.
3. If applicable, click **Yes**.

The host is in maintenance mode until you select **Maintenance Mode** > **Exit Maintenance Mode**.

Remove a Host from a Cluster

You can remove hosts from a cluster.

1. Browse to the host in the vSphere Client.
2. Right-click the host and select **Maintenance Mode** > **Enter Maintenance Mode**.

   When the host is in maintenance mode, move it to a different inventory location, either the top-level data center or to a different cluster.
3. Right-click the host and select **Move To...**.
4. Select a new location for the host and click **OK**.

When you move the host, its resources are removed from the cluster. If you grafted the host's resource pool hierarchy onto the cluster, that hierarchy remains with the cluster.

After you remove a host from a cluster, you can perform the following tasks.

- Remove the host from vCenter Server.
- Run the host as a standalone host under vCenter Server.
- Move the host into another cluster.

Using Standby Mode

When a host machine is placed in standby mode, it is powered off.

Normally, hosts are placed in standby mode by the vSphere DPM feature to optimize power usage. You can also place a host in standby mode manually. However, DRS might undo (or recommend undoing) your change the next time it runs. To force a host to remain off, place it in maintenance mode and power it off.

DRS Cluster Validity

The vSphere Client indicates whether a DRS cluster is valid, overcommitted (yellow), or invalid (red).

DRS clusters become overcommitted or invalid for several reasons.

- A cluster might become overcommitted if a host fails.

- A cluster becomes invalid if vCenter Server is unavailable and you power on virtual machines using the vSphere Client.
- A cluster becomes invalid if the user reduces the reservation on a parent resource pool while a virtual machine is in the process of failing over.
- If changes are made to hosts or virtual machines using the vSphere Client while vCenter Server is unavailable, those changes take effect. When vCenter Server becomes available again, you might find that clusters have turned red or yellow because cluster requirements are no longer met.

When considering cluster validity scenarios, you should understand these terms.

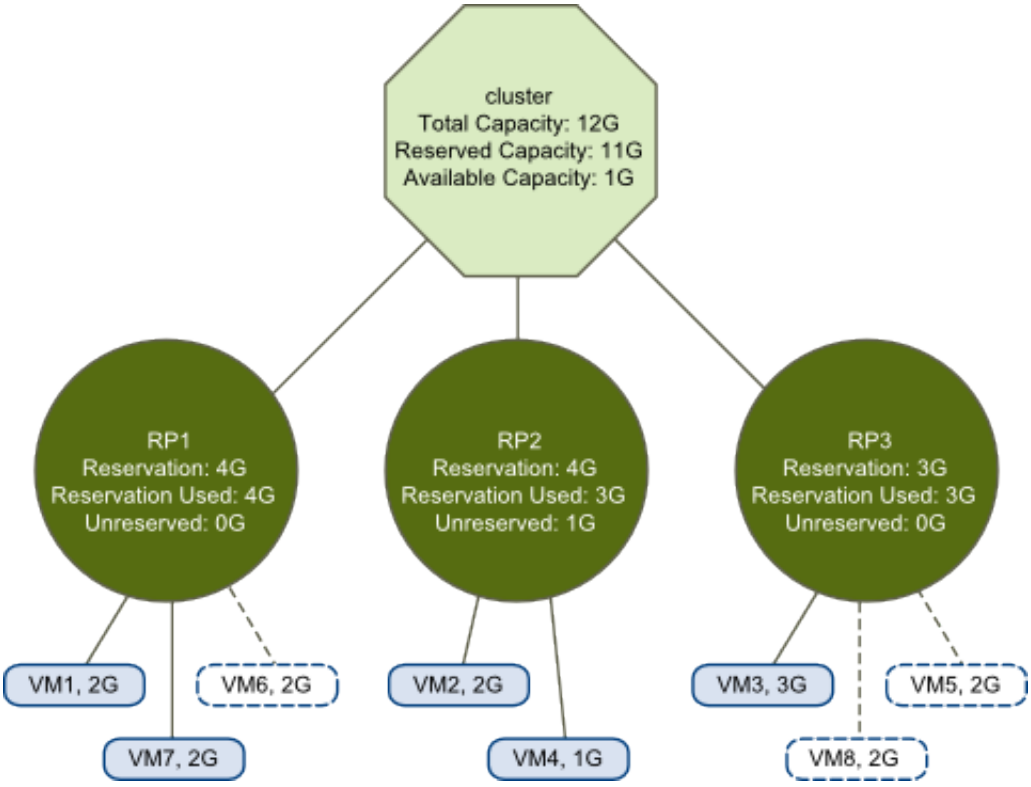
Reservation	A fixed, guaranteed allocation for the resource pool input by the user.
Reservation Used	The sum of the reservation or reservation used (whichever is larger) for each child resource pool, added recursively.
Unreserved	This nonnegative number differs according to resource pool type. • Nonexpandable resource pools: Reservation minus reservation used. • Expandable resource pools: (Reservation minus reservation used) plus any unreserved resources that can be borrowed from its ancestor resource pools.

Valid DRS Clusters

A valid cluster has enough resources to meet all reservations and to support all running virtual machines.

The following figure shows an example of a valid cluster with fixed resource pools and how its CPU and memory resources are computed.

Figure 105: Valid Cluster with Fixed Resource Pools

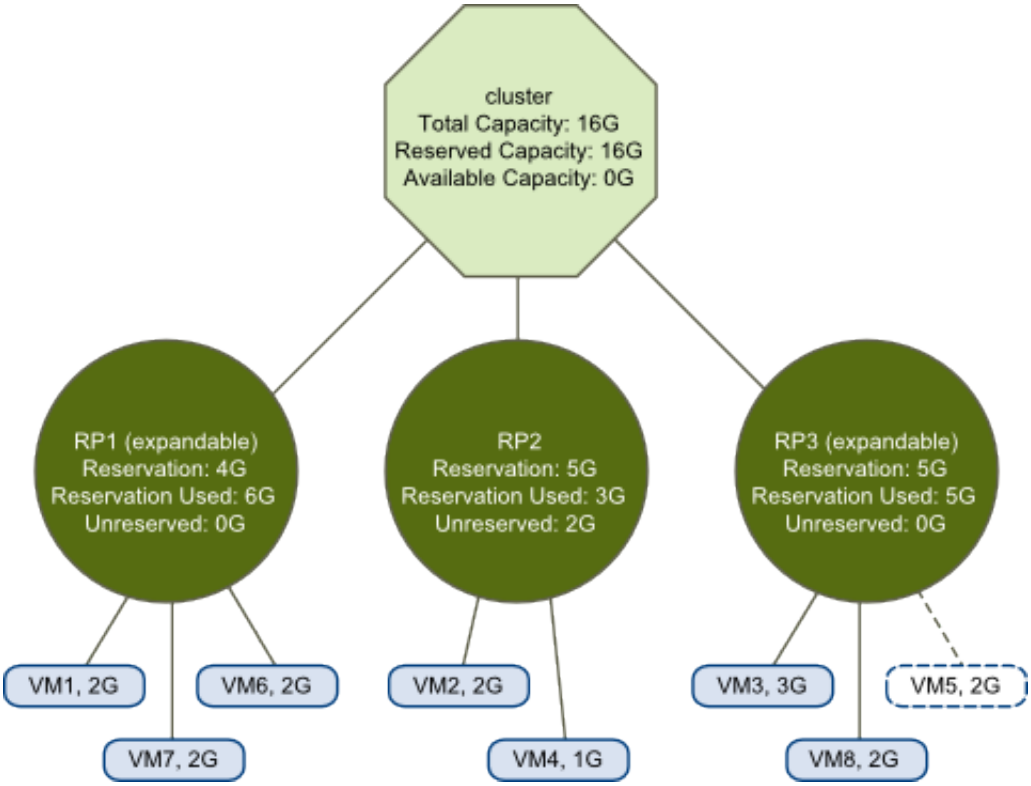


The cluster has the following characteristics:

- A cluster with total resources of 12GHz.
- Three resource pools, each of type **Fixed** (**Expandable Reservation** is not selected).
- The total reservation of the three resource pools combined is 11GHz (4+4+3 GHz). The total is shown in the **Reserved Capacity** field for the cluster.
- RP1 was created with a reservation of 4GHz. Two virtual machines. (VM1 and VM7) of 2GHz each are powered on (**Reservation Used**: 4GHz). No resources are left for powering on additional virtual machines. VM6 is shown as not powered on. It consumes none of the reservation.
- RP2 was created with a reservation of 4GHz. Two virtual machines of 1GHz and 2GHz are powered on (**Reservation Used**: 3GHz). 1GHz remains unreserved.
- RP3 was created with a reservation of 3GHz. One virtual machine with 3GHz is powered on. No resources for powering on additional virtual machines are available.

The following figure shows an example of a valid cluster with some resource pools (RP1 and RP3) using reservation type **Expandable**.

Figure 106: Valid Cluster with Expandable Resource Pools



A valid cluster can be configured as follows:

- A cluster with total resources of 16GHz.
- RP1 and RP3 are of type **Expandable**, RP2 is of type Fixed.
- The total reservation used of the three resource pools combined is 16GHz (6GHz for RP1, 5GHz for RP2, and 5GHz for RP3). 16GHz shows up as the **Reserved Capacity** for the cluster at top level.
- RP1 was created with a reservation of 4GHz. Three virtual machines of 2GHz each are powered on. Two of those virtual machines (for example, VM1 and VM7) can use RP1's reservations, the third virtual machine (VM6) can use reservations from the cluster's resource pool. (If the type of this resource pool were **Fixed**, you could not power on the additional virtual machine.)

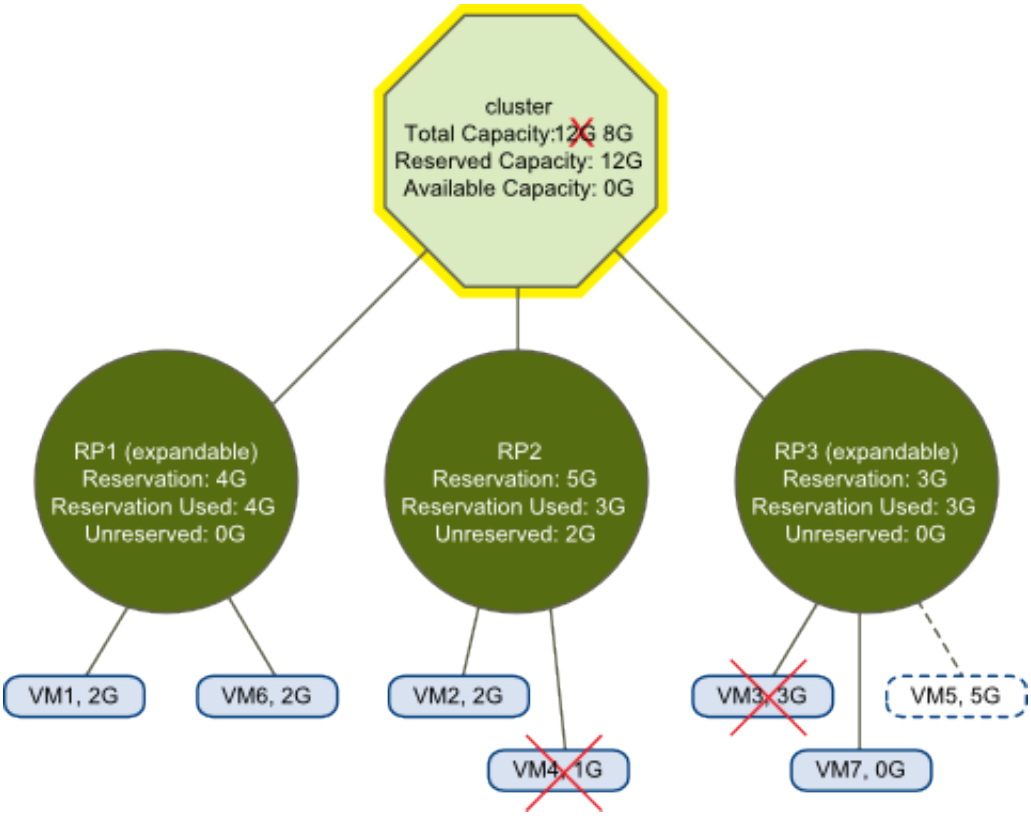
- RP2 was created with a reservation of 5GHz. Two virtual machines of 1GHz and 2GHz are powered on (**Reservation Used**: 3GHz). 2GHz remains unreserved.
  RP3 was created with a reservation of 5GHz. Two virtual machines of 3GHz and 2GHz are powered on. Even though this resource pool is of type **Expandable**, no additional 2GHz virtual machine can be powered on because the parent's extra resources are already used by RP1.

Overcommitted DRS Clusters

A cluster becomes overcommitted (yellow) when the tree of resource pools and virtual machines is internally consistent but the cluster does not have the capacity to support all resources reserved by the child resource pools.

There will always be enough resources to support all running virtual machines because, when a host becomes unavailable, all its virtual machines become unavailable. A cluster typically turns yellow when cluster capacity is suddenly reduced, for example, when a host in the cluster becomes unavailable. VMware recommends that you leave adequate additional cluster resources to avoid your cluster turning yellow.

Figure 107: Yellow Cluster



In this example:

- A cluster with total resources of 12GHz coming from three hosts of 4GHz each.
- Three resource pools reserving a total of 12GHz.
- The total reservation used by the three resource pools combined is 12GHz (4+5+3 GHz). That shows up as the **Reserved Capacity** in the cluster.
- One of the 4GHz hosts becomes unavailable, so total resources reduce to 8GHz.
- At the same time, VM4 (1GHz) and VM3 (3GHz), which were running on the host that failed, are no longer running.

- The cluster is now running virtual machines that require a total of 6GHz. The cluster still has 8GHz available, which is sufficient to meet virtual machine requirements.
  The resource pool reservations of 12GHz can no longer be met, so the cluster is marked as yellow.

Invalid DRS Clusters

A cluster enabled for DRS becomes invalid (red) when the tree is no longer internally consistent, that is, resource constraints are not observed.

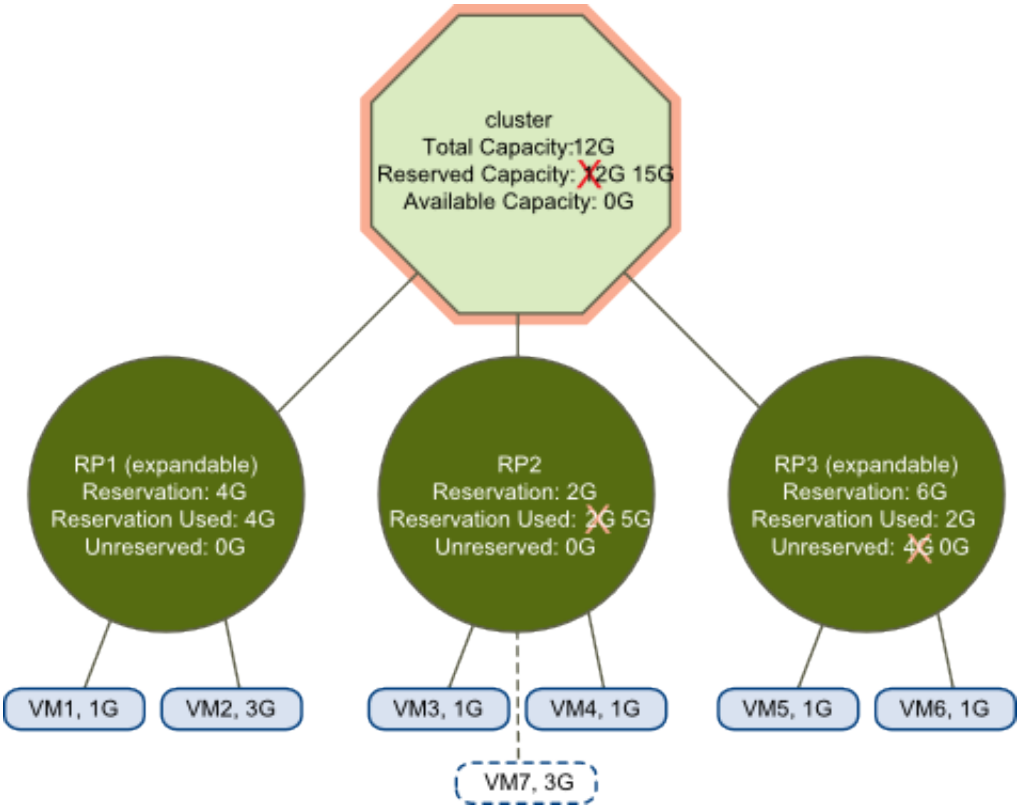
The total amount of resources in the cluster does not affect whether the cluster is red. A cluster can be red, even if enough resources exist at the root level, if there is an inconsistency at a child level.

You can resolve a red DRS cluster problem either by powering off one or more virtual machines, moving virtual machines to parts of the tree that have sufficient resources, or editing the resource pool settings in the red part. Adding resources typically helps only when you are in the yellow state.

A cluster can also turn red if you reconfigure a resource pool while a virtual machine is failing over. A virtual machine that is failing over is disconnected and does not count toward the reservation used by the parent resource pool. You might reduce the reservation of the parent resource pool before the failover completes. After the failover is complete, the virtual machine resources are again charged to the parent resource pool. If the pool's usage becomes larger than the new reservation, the cluster turns red.

If a user is able to start a virtual machine (in an unsupported way) with a reservation of 3GHz under resource pool 2, the cluster would become red, as shown in the following figure.

Figure 108: Red Cluster



Managing Power Resources

The vSphere Distributed Power Management (DPM) feature allows a DRS cluster to reduce its power consumption by powering hosts on and off based on cluster resource utilization.

vSphere DPM monitors the cumulative demand of all virtual machines in the cluster for memory and CPU resources and compares this to the total available resource capacity of all hosts in the cluster. If sufficient excess capacity is found, vSphere DPM places one or more hosts in standby mode and powers them off after migrating their virtual machines to other hosts. Conversely, when capacity is deemed to be inadequate, DRS brings hosts out of standby mode (powers them on) and uses vMotion to migrate virtual machines to them. When making these calculations, vSphere DPM considers not only current demand, but it also honors any user-specified virtual machine resource reservations.

If you enable **Forecasted Metrics** when you create a DRS cluster, DPM will issue proposals in advance depending on the rolling forecast window you select.

Note: ESXi hosts cannot automatically be brought out of standby mode unless they are running in a cluster managed by vCenter Server.

vSphere DPM can use one of three power management protocols to bring a host out of standby mode: Intelligent Platform Management Interface (IPMI), Hewlett-Packard Integrated Lights-Out (iLO), or Wake-On-LAN (WOL). Each protocol requires its own hardware support and configuration. If a host does not support any of these protocols it cannot be put into standby mode by vSphere DPM. If a host supports multiple protocols, they are used in the following order: IPMI, iLO, WOL.

Note: Do not disconnect a host in standby mode or move it out of the DRS cluster without first powering it on, otherwise vCenter Server is not able to power the host back on.

Configure IPMI or iLO Settings for vSphere DPM

IPMI is a hardware-level specification and Hewlett-Packard iLO is an embedded server management technology. Each of them describes and provides an interface for remotely monitoring and controlling computers.

Both IPMI and iLO require a hardware Baseboard Management Controller (BMC) to provide a gateway for accessing hardware control functions, and allow the interface to be accessed from a remote system using serial or LAN connections. The BMC is powered-on even when the host itself is powered-off. If properly enabled, the BMC can respond to remote power-on commands.

If you plan to use IPMI or iLO as a wake protocol, you must configure the BMC. BMC configuration steps vary according to model. See your vendor’s documentation for more information. With IPMI, you must also ensure that the BMC LAN channel is configured to be always available and to allow operator-privileged commands. On some IPMI systems, when you enable "IPMI over LAN" you must configure this in the BIOS and specify a particular IPMI account.

vSphere DPM using only IPMI supports MD5- and plaintext-based authentication, but MD2-based authentication is not supported. vCenter Server uses MD5 if a host's BMC reports that it is supported and enabled for the Operator role.

Otherwise, plaintext-based authentication is used if the BMC reports it is supported and enabled. If neither MD5 nor plaintext authentication is enabled, IPMI cannot be used with the host and vCenter Server attempts to use Wake-on-LAN.

You must perform the following procedure on each host.

1. Browse to the host in the vSphere Client.
2. Click the **Configure** tab.
3. Under **System**, click **Power Management**.
4. Click **Edit**.
5. Enter the following information.
   - User name and password for a BMC account. (The user name must have the ability to remotely power the host on.)
   - IP address of the NIC associated with the BMC, as distinct from the IP address of the host. The IP address should be static or a DHCP address with infinite lease.
   - MAC address of the NIC associated with the BMC.
6. Click **OK**.

Test Wake-on-LAN for vSphere DPM

The use of Wake-on-LAN (WOL) for the vSphere DPM feature is fully supported, if you configure and successfully test it according to the VMware guidelines. You must perform these steps before activating vSphere DPM for a cluster for the first time or on any host that is being added to a cluster that is using vSphere DPM.

Before testing WOL, ensure that your cluster meets the prerequisites.

- Your cluster must contain at least two hosts that are version ESX 3.5 (or ESX 3i version 3.5) or later.
- Each host's vMotion networking link must be working correctly. The vMotion network should also be a single IP subnet, not multiple subnets separated by routers.
- The vMotion NIC on each host must support WOL. To check for WOL support, first determine the name of the physical network adapter corresponding to the VMkernel port by selecting the host in the inventory panel of the vSphere Client, selecting the **Configuration** tab, and clicking **Networking**. After you have this information, click on **Network Adapters** and find the entry corresponding to the network adapter. The **Wake On LAN Supported** column for the relevant adapter should show Yes.
- To display the WOL-compatibility status for each NIC on a host, select the host in the inventory panel of the vSphere Client, select the **Configuration** tab, and click **Network Adapters**. The NIC must show Yes in the **Wake On LAN Supported** column.
- The switch port that each WOL-supporting vMotion NIC is plugged into should be set to auto negotiate the link speed, and not set to a fixed speed (for example, 1000 Mb/s). Many NICs support WOL only if they can switch to 100 Mb/s or less when the host is powered off.

After you verify these prerequisites, test each ESXi host that is going to use WOL to support vSphere DPM. When you test these hosts, ensure that the vSphere DPM feature is deactivated for the cluster.

CAUTION: Ensure that any host being added to a vSphere DPM cluster that uses WOL as a wake protocol is tested and deactivated from using power management if it fails the testing. If this is not done, vSphere DPM might power off hosts that it subsequently cannot power back up.

1. Browse to the host in the vSphere Client.
2. Right-click the host and select **Power** > **Enter Standby Mode**

   This action powers down the host.

3. Right-click the host and select **Power** > **Power On** to attempt to bring it out of standby mode.
4. Observe whether or not the host successfully powers back on.
5. For any host that fails to exit standby mode successfully, perform the following steps.
   a) Select the host in the vSphere Client and select the **Configure** tab.
   b) Under **Hardware** > **Power Management**, click **Edit** to adjust the power management policy.

   After you do this, vSphere DPM does not consider that host a candidate for being powered off.

Activating vSphere DPM for a DRS Cluster

After you have performed configuration or testing steps required by the wake protocol you are using on each host, you can enable vSphere DPM.

Configure the power management automation level, threshold, and host-level overrides. These settings are configured under **Power Management** in the cluster's Settings dialog box.

You can also create scheduled tasks to enable and deactivate DPM for a cluster using the **Schedule Task: Change Cluster Power Settings** wizard.

Note: If a host in your DRS cluster has USB devices connected, deactivate DPM for that host. Otherwise, DPM might turn off the host and sever the connection between the device and the virtual machine that was using it.

Automation Level

Whether the host power state and migration recommendations generated by vSphere DPM are run automatically or not depends upon the power management automation level selected for the feature.

The automation level is configured under **Power Management** in the cluster's Settings dialog box.

Note: The power management automation level is not the same as the DRS automation level.

Table 336: Power Management Automation Level

Option	Description
Off	The feature is deactivated and no recommendations are made.
Manual	Host power operation and related virtual machine migration recommendations are made, but not automatically run.
Automatic	Host power operations are automatically run if related virtual machine migrations can all be run automatically.

vSphere DPM Threshold

The power state (host power on or off) recommendations generated by the vSphere DPM feature are assigned priorities that range from priority-one recommendations to priority-five recommendations.

These priority ratings are based on the amount of over- or under-utilization found in the DRS cluster and the improvement that is expected from the intended host power state change. A priority-one recommendation is mandatory, while a priority-five recommendation brings only slight improvement.

The threshold is configured under **Power Management** in the cluster's Settings dialog box. Each level you move the vSphere DPM Threshold slider to the right allows the inclusion of one more lower level of priority in the set of recommendations that are executed automatically or appear as recommendations to be manually executed. At the Conservative setting, vSphere DPM only generates priority-one recommendations, the next level to the right only priority-

two and higher, and so on, down to the Aggressive level which generates priority-five recommendations and higher (that is, all recommendations.)

Note: The DRS threshold and the vSphere DPM threshold are essentially independent. You can differentiate the aggressiveness of the migration and host-power-state recommendations they respectively provide.

Host-Level Overrides

When you activate vSphere DPM in a DRS cluster, by default all hosts in the cluster inherit its vSphere DPM automation level.

You can override this default for an individual host by selecting the Host Options page of the cluster's Settings dialog box and clicking its **Power Management** setting. You can change this setting to the following options:

- Disabled
- Manual
- Automatic

Note: Do not change a host's Power Management setting if it has been set to Disabled due to failed exit standby mode testing.

After activating and running vSphere DPM, you can verify that it is functioning properly by viewing each host's **Last Time Exited Standby** information displayed on the Host Options page in the cluster Settings dialog box and on the **Hosts** tab for each cluster. This field shows a timestamp and whether vCenter Server Succeeded or Failed the last time it attempted to bring the host out of standby mode. If no such attempt has been made, the field displays Never.

Note: Times for the **Last Time Exited Standby** text box are derived from the vCenter Server event log. If this log is cleared, the times are reset to Never.

Monitoring vSphere DPM

You can use event-based alarms in vCenter Server to monitor vSphere DPM.

The most serious potential error you face when using vSphere DPM is the failure of a host to exit standby mode when its capacity is needed by the DRS cluster. You can monitor for instances when this error occurs by using the preconfigured **Exit Standby Error** alarm in vCenter Server. If vSphere DPM cannot bring a host out of standby mode (vCenter Server event `DrsExitStandbyModeFailedEvent`), you can configure this alarm to send an alert email to the administrator or to send notification using an SNMP trap. By default, this alarm is cleared after vCenter Server is able to successfully connect to that host.

To monitor vSphere DPM activity, you can also create alarms for the following vCenter Server events.

Table 337: vCenter Server Events

Event Type	Event Name
Entering Standby mode (about to power off host)	`DrsEnteringStandbyModeEvent`
Successfully entered Standby mode (host power off succeeded)	`DrsEnteredStandbyModeEvent`
Exiting Standby mode (about to power on the host)	`DrsExitingStandbyModeEvent`
Successfully exited Standby mode (power on succeeded)	`DrsExitedStandbyModeEvent`

For more information about creating and editing alarms, see the *vSphere Monitoring and Performance* documentation.

If you use monitoring software other than vCenter Server, and that software triggers alarms when physical hosts are powered off unexpectedly, you might have a situation where false alarms are generated when vSphere DPM places a host

into standby mode. If you do not want to receive such alarms, work with your vendor to deploy a version of the monitoring software that is integrated with vCenter Server. You could also use vCenter Server itself as your monitoring solution, because starting with vSphere 4.x, it is inherently aware of vSphere DPM and does not trigger these false alarms.

Using Affinity Rules with vSphere DRS

You can control the placement of virtual machines on hosts within a cluster by using affinity rules.

Note: This topic describes using affinity rules with DRS. You can also use affinity rules without DRS.

You can create two types of rules.

- Used to specify affinity or anti-affinity between a group of virtual machines and a group of hosts. An affinity rule specifies that the members of a selected virtual machine DRS group can or must run on the members of a specific host DRS group. An anti-affinity rule specifies that the members of a selected virtual machine DRS group cannot run on the members of a specific host DRS group.
  See VM-Host Affinity Rules with vSphere DRS for information about creating and using this type of rule.
- Used to specify affinity or anti-affinity between individual virtual machines. A rule specifying affinity causes DRS to try to keep the specified virtual machines together on the same host, for example, for performance reasons. With an anti-affinity rule, DRS tries to keep the specified virtual machines apart, for example, so that when a problem occurs with one host, you do not lose both virtual machines.
  See VM-VM Affinity Rules with vSphere DRS for information about creating and using this type of rule.

When you add or edit an affinity rule, and the cluster's current state is in violation of the rule, the system continues to operate and tries to correct the violation. For manual and partially automated DRS clusters, migration recommendations based on rule fulfillment and load balancing are presented for approval. You are not required to fulfill the rules, but the corresponding recommendations remain until the rules are fulfilled.

To check whether any enabled affinity rules are being violated and cannot be corrected by DRS, select the cluster's **DRS** tab and click **Faults**. Any rule currently being violated has a corresponding fault on this page. Read the fault to determine why DRS is not able to satisfy the particular rule. Rules violations also produce a log event.

Note: VM-VM and VM-Host affinity rules are different from an individual host’s CPU affinity rules.

VM-VM Affinity Rules with vSphere DRS

A VM-VM affinity rule with DRS specifies whether selected individual virtual machines should run on the same host or be kept on separate hosts. This type of rule is used to create affinity or anti-affinity between individual virtual machines that you select.

Note: This topic describes using affinity rules with DRS. You can also use affinity rules without DRS.

When an affinity rule is created, DRS tries to keep the specified virtual machines together on the same host. You might want to do this, for example, for performance reasons.

With an anti-affinity rule, DRS tries to keep the specified virtual machines apart. You could use such a rule if you want to guarantee that certain virtual machines are always on different physical hosts. In that case, if a problem occurs with one host, not all virtual machines would be placed at risk.

VM-Host Affinity Rules with vSphere DRS

A VM-Host affinity rule specifies whether or not the members of a selected virtual machine DRS group can run on the members of a specific host DRS group.

Note: This topic describes using affinity rules for DRS. You can also use affinity rules without DRS.

Unlike a VM-VM affinity rule, which specifies affinity (or anti-affinity) between individual virtual machines, a VM-Host affinity rule specifies an affinity relationship between a group of virtual machines and a group of hosts. There are 'required' rules (designated by "must") and 'preferential' rules (designated by "should".)

A VM-Host affinity rule includes the following components.

- One virtual machine DRS group.
- One host DRS group.
- A designation of whether the rule is a requirement ("must") or a preference ("should") and whether it is affinity ("run on") or anti-affinity ("not run on").

Because VM-Host affinity rules are cluster-based, the virtual machines and hosts that are included in a rule must all reside in the same cluster. If a virtual machine is removed from the cluster, it loses its DRS group affiliation, even if it is later returned to the cluster.

Create a VM-Host Group

A VM-Host affinity rule establishes an affinity (or anti-affinity) relationship between a virtual machine group with a host group. You must create both of these groups before you can create a rule that links them.

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab.
3. Under **Configuration**, select **VM/Host Groups** and click **Add**.
4. In the **Create VM/Host Group** dialog box, type a name for the group.
5. Select **Host Group** from the **Type** drop down box and click **Add**.
6. Click the check box next to a host to add it. Continue this process until all desired hosts have been added.
7. Click **OK**.

Using this host group, you can create a VM-Host affinity rule that establishes an affinity (or anti-affinity) relationship with an appropriate virtual machine group.

Create a Virtual Machine Group

Affinity rules establish an affinity (or anti-affinity) relationship between groups. You must create groups before you can create a rule that links them.

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab.
3. Under **Configuration**, select **VM/Host Groups** and click **Add**.
4. In the **Create VM/Host Group** dialog box, type a name for the group.
5. Select **VM Group** from the **Type** drop down box and click **Add**.
6. Click the check box next to a virtual machine to add it. Continue this process until all desired virtual machines have been added.
7. Click **OK**.

Create a VM-VM Affinity Rule

You can create VM-VM affinity rules to specify whether selected individual virtual machines should run on the same host or be kept on separate hosts.

Note: If you use the vSphere HA Specify Failover Hosts admission control policy and designate multiple failover hosts, VM-VM affinity rules are not supported.

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab.
3. Under **Configuration**, click **VM/Host Rules**.
4. Click **Add**.
5. In the **Create VM/Host Rule** dialog box, type a name for the rule.
6. From the **Type** drop-down menu, select either **Keep Virtual Machines Together** or **Separate Virtual Machines**.
7. Click **Add**.
8. Select at least two virtual machines to which the rule will apply and click **OK**.
9. Click **OK**.

VM-VM Affinity Rule Conflicts

You can create and use multiple VM-VM affinity rules, however, this might lead to situations where the rules conflict with one another.

If two VM-VM affinity rules are in conflict, you cannot activate both. For example, if one rule keeps two virtual machines together and another rule keeps the same two virtual machines apart, you cannot activate both rules. Select one of the rules to apply and deactivate or remove the conflicting rule.

When two VM-VM affinity rules conflict, the older one takes precedence and the newer rule is deactivated. DRS only tries to satisfy activated rules and deactivated rules are ignored. DRS gives higher precedence to preventing violations of anti-affinity rules than violations of affinity rules.

Create a VM-Host Affinity Rule

You can create VM-Host affinity rules to specify whether or not the members of a selected virtual machine group can run on the members of a specific host group.

Create the virtual machine and host groups to which the VM-Host affinity rule applies.

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab.
3. Under **Configuration**, click **VM/Host Rules**.
4. Click **Add**.
5. In the **Create VM/Host Rule** dialog box, type a name for the rule.
6. From the **Type** drop down menu, select **Virtual Machines to Hosts**.
7. Select the virtual machine group and the host group to which the rule applies.
8. Select a specification for the rule.
   - **Must run on hosts in group**. Virtual machines in VM Group 1 must run on hosts in Host Group A.
   - **Should run on hosts in group**. Virtual machines in VM Group 1 should, but are not required, to run on hosts in Host Group A.
   - **Must not run on hosts in group**. Virtual machines in VM Group 1 must never run on host in Host Group A.
   - **Should not run on hosts in group**. Virtual machines in VM Group 1 should not, but might, run on hosts in Host Group A.
9. Click **OK**.

Using VM-Host Affinity Rules

You use a VM-Host affinity rule to specify an affinity relationship between a group of virtual machines and a group of hosts. When using VM-Host affinity rules, you should be aware of when they could be most useful, how conflicts between rules are resolved, and the importance of caution when setting required affinity rules.

If you create more than one VM-Host affinity rule, the rules are not ranked, but are applied equally. Be aware that this has implications for how the rules interact. For example, a virtual machine that belongs to two groups, each of which belongs to a different required rule, can run only on hosts that belong to both of the host groups represented in the rules.

When you create a VM-Host affinity rule, its ability to function in relation to other rules is not checked. So it is possible for you to create a rule that conflicts with the other rules you are using. When two VM-Host affinity rules conflict, the older one takes precedence and the newer rule is deactivated. DRS only tries to satisfy activated rules and deactivated rules are ignored.

DRS, vSphere HA, and vSphere DPM never take any action that results in the violation of required affinity rules (those where the virtual machine group 'must run on' or 'must not run on' the host group). Accordingly, you should exercise caution when using this type of rule because of its potential to adversely affect the functioning of the cluster. If improperly used, required VM-Host affinity rules can fragment the cluster and inhibit the proper functioning of DRS, vSphere HA, and vSphere DPM.

A number of cluster functions are not performed if doing so would violate a required affinity rule.

- DRS does not evacuate virtual machines to place a host in maintenance mode.
- DRS does not place virtual machines for power-on or load balance virtual machines.
- vSphere HA does not perform failovers.
- vSphere DPM does not optimize power management by placing hosts into standby mode.

To avoid these situations, exercise caution when creating more than one required affinity rule or consider using VM-Host affinity rules that are preferential only (those where the virtual machine group 'should run on' or 'should not run on' the host group). Ensure that the number of hosts in the cluster with which each virtual machine is affined is large enough that losing a host does not result in a lack of hosts on which the virtual machine can run. Preferential rules can be violated to allow the proper functioning of DRS, vSphere HA, and vSphere DPM.

Note: You can create an event-based alarm that is triggered when a virtual machine violates a VM-Host affinity rule. Add a new alarm for the virtual machine and select **VM is violating VM-Host Affinity Rule** as the event trigger. For more information about creating and editing alarms, see the vSphere Monitoring and Performance documentation.

Using Affinity Rules without vSphere DRS

You can use affinity rules without using vSphere DRS.

VM affinity rules allow you to control the placement of VMs within a vSphere cluster. VM-VM affinity means the VMs must be run on the same host within a cluster. Workloads are comprised of multiple VMs that have dependencies on each other. Using **Keep Virtual Machines Together** rules ensure that all selected VMs run on the same host.

VM-VM anti-affinity means the VMs must be run on different hosts within a cluster. You can use a **Separate Virtual Machines** rule when you have multiple resource intensive VMs to ensure that these VMs are always running on different hosts in the cluster to avoid resource contention.

VM-Host affinity rules control the VM to Host relationship and has 4 sub-rules. Use cases for VM-Host rules would include making sure workloads run (or do not run) on specific hosts in a mixed-hardware cluster. For licensing reasons, you may need to ensure that an application only runs on a specific host or specific subset of hosts.

The VM-Host rules leverage VM-Host groups. A VM group is a user-defined group of one or more VMs. A host group is a user-defined group of one or more hosts.

Rule	Description	Persistence
Must run on hosts in group	The VM group must be run on the defined host group.	A hard rule that cannot be violated.
Must not run on hosts in group	The VM group must not be run on the defined host group.	A hard rule that cannot be violated.
Should run on hosts in group	The VM group should be run on the defined host group.	A soft rule that can be violated.
Should not run on hosts in group	The VM group should not be run on the defined host group.	A soft rule that can be violated.

VM-Host groups and VM-Host rules can be created, deleted, and edited when vSphere DRS is not activated. The interface to manage VM-Host groups and VM-Host rules exists outside of the vSphere DRS configuration.

In the event of a vSphere HA failover of VMs, affinity rules are respected. This is true for rule types **Keep Virtual Machines Together** and **Separate Virtual Machines**, as well as hard VM-Host rule types. vSphere HA is unable to failover VMs if a hard rule would be violated. When using soft VM-Host rules, vSphere HA operations succeed even if the rule is violated. Soft rules allow for violation of their definitions.

For example, a 2-node cluster and a **Separate Virtual Machines** rule defined to place VM-1 on ESX-01 and VM-2 on ESX-02. ESX-01 experiences a failure and vSphere HA is initiated. vSphere HA is unable to power on VM-1 on ESX-02 as it would violate the rule to keep each virtual machine separate.

VM power on operations do not allow affinity rules to be violated. This is true for rule types **Keep Virtual Machines Together** and **Separate Virtual Machines**, as well as hard VM-Host rules. When using soft VM-Host rules, power on operations succeed even if the rule is violated. Soft rules allow for violation of their definitions.

For example, if a rule is defined to **Keep Virtual Machines Together** on VM-1 and VM-2 and VM-1 is currently already powered on, an attempt to power on VM-2 will fail if it is registered to a different host. Since vSphere DRS is not activated, the user must manually migrate the VMs to the same host to be able to power on the VM.

When vSphere DRS is not activated and therefore not automatically migrating VMs, you can initiate migrations using vSphere vMotion on VMs with affinity rules defined. Both rule types **Keep Virtual Machines Together** and **Separate**

Virtual Machines can be violated by migrating using vSphere vMotion. For example, if a rule is defined to **Separate Virtual Machines** on VM-1 and VM-2, an attempt to migrate the VMs to the same host will not be blocked. The operation will succeed even though it would violate the rule.

Any hard VM-Host rule cannot be violated by a user-initiated migration. For example, if a rule is defined that VM-1 and VM-2 must run on hosts ESX-01 and ESX-02, an attempt to migrate the VMs to hosts outside of the host group is blocked.

Soft VM-Host rules can be violated by a user-initiated migration. Soft rules allow for violation of their definitions. For example, if a rule is defined that VM-1 and VM-2 should not run on hosts ESX-03 and ESX-04, an attempt to migrate the VMs to either ESX-03 or ESX-04 is not blocked.

When vSphere DRS is not activated, there is no automatic remediation of VM placement. This includes violations because of manual migrations and violations that occur if new rules are defined that would violate current VM placement. Without vSphere DRS, you must correct VM placement to comply with rules.

Creating a Datastore Cluster

A datastore cluster is a collection of datastores with shared resources and a shared management interface. Datastore clusters are to datastores what clusters are to hosts. When you create a datastore cluster, you can use vSphere Storage DRS to manage storage resources.

Note: Datastore clusters are referred to as storage pods in the vSphere API.

When you add a datastore to a datastore cluster, the datastore's resources become part of the datastore cluster's resources. As with clusters of hosts, you use datastore clusters to aggregate storage resources, which enables you to support resource allocation policies at the datastore cluster level. The following resource management capabilities are also available per datastore cluster.

Space utilization load balancing	You can set a threshold for space use. When space use on a datastore exceeds the threshold, Storage DRS generates recommendations or performs Storage vMotion migrations to balance space use across the datastore cluster.
I/O latency load balancing	You can set an I/O latency threshold for bottleneck avoidance. When I/O latency on a datastore exceeds the threshold, Storage DRS generates recommendations or performs Storage vMotion migrations to help alleviate high I/O load.
Anti-affinity rules	You can create anti-affinity rules for virtual machine disks. For example, the virtual disks of a certain virtual machine must be kept on different datastores. By default, all virtual disks for a virtual machine are placed on the same datastore.

Initial Placement and Ongoing Balancing

Storage DRS provides initial placement and ongoing balancing recommendations to datastores in a Storage DRS-enabled datastore cluster.

Initial placement occurs when Storage DRS selects a datastore within a datastore cluster on which to place a virtual machine disk. This happens when the virtual machine is being created or cloned, when a virtual machine disk is being migrated to another datastore cluster, or when you add a disk to an existing virtual machine.

Initial placement recommendations are made in accordance with space constraints and with respect to the goals of space and I/O load balancing. These goals aim to minimize the risk of over-provisioning one datastore, storage I/O bottlenecks, and performance impact on virtual machines.

Storage DRS is invoked at the configured frequency (by default, every eight hours) or when one or more datastores in a datastore cluster exceeds the user-configurable space utilization thresholds. When Storage DRS is invoked, it checks each datastore's space utilization and I/O latency values against the threshold. For I/O latency, Storage DRS uses the 90th percentile I/O latency measured over the course of a day to compare against the threshold.

Storage Migration Recommendations

vCenter Server displays migration recommendations on the Storage DRS Recommendations page for datastore clusters that have manual automation mode.

The system provides as many recommendations as necessary to enforce Storage DRS rules and to balance the space and I/O resources of the datastore cluster. Each recommendation includes the virtual machine name, the virtual disk name, the name of the datastore cluster, the source datastore, the destination datastore, and a reason for the recommendation.

- Balance datastore space use
- Balance datastore I/O load

Storage DRS makes mandatory recommendations for migration in the following situations:

- The datastore is out of space.
- Anti-affinity or affinity rules are being violated.
- The datastore is entering maintenance mode and must be evacuated.

In addition, optional recommendations are made when a datastore is close to running out of space or when adjustments should be made for space and I/O load balancing.

Storage DRS considers moving virtual machines that are powered off or powered on for space balancing. Storage DRS includes powered-off virtual machines with snapshots in these considerations.

Create a Datastore Cluster

You can manage datastore cluster resources using Storage DRS.

1. Browse to data centers in the vSphere Client.
2. Right-click the data center and select **Storage**, **New Datastore Cluster**.
3. To complete the **New Datastore Cluster** wizard, follow the prompts.
4. Click **Finish**.

Activate and Deactivate Storage DRS

Storage DRS allows you to manage the aggregated resources of a datastore cluster. When Storage DRS is activated, it provides recommendations for virtual machine disk placement and migration to balance space and I/O resources across the datastores in the datastore cluster.

When you activate Storage DRS, you activate the following functions.

- Space load balancing among datastores within a datastore cluster.
- I/O load balancing among datastores within a datastore cluster.
- Initial placement for virtual disks based on space and I/O workload.

The Enable Storage DRS check box in the Datastore Cluster Settings dialog box activates or deactivates all of these components at once. If necessary, you can deactivate I/O-related functions of Storage DRS independently of space balancing functions.

When you deactivate Storage DRS on a datastore cluster, Storage DRS settings are preserved. When you activate Storage DRS, the settings for the datastore cluster are restored to the point where Storage DRS was deactivated.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Select **Storage DRS** and click **Edit**.
4. Select **Turn ON vSphere DRS** and click **OK**.
5. Optional: To deactivate only I/O-related functions of Storage DRS, leaving space-related controls activated, perform the following steps.
   a) Under **Storage DRS** select **Edit**.
   b) Deselect the **Enable I/O metric for Storage DRS** check box and click **OK**.

Set the Automation Level for Datastore Clusters

The automation level for a datastore cluster specifies whether or not placement and migration recommendations from Storage DRS are applied automatically.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Select **DRS** and click **Edit**.
4. Expand DRS Automation and select an automation level.

   Manual is the default automation level.

Option	Description
No Automation (Manual Mode)	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.

5. Click **OK**.

Setting the Aggressiveness Level for Storage DRS

The aggressiveness of Storage DRS is determined by specifying thresholds for space used and I/O latency.

Storage DRS collects resource usage information for the datastores in a datastore cluster. vCenter Server uses this information to generate recommendations for placement of virtual disks on datastores.

When you set a low aggressiveness level for a datastore cluster, Storage DRS recommends Storage vMotion migrations only when absolutely necessary, for example, if when I/O load, space utilization, or their imbalance is high. When you set a high aggressiveness level for a datastore cluster, Storage DRS recommends migrations whenever the datastore cluster can benefit from space or I/O load balancing.

In the vSphere Client, you can use the following thresholds to set the aggressiveness level for Storage DRS:

Space Utilization
: Storage DRS generates recommendations or performs migrations when the percentage of space utilization on the datastore is greater than the threshold you set in the vSphere Client.

I/O Latency
: Storage DRS generates recommendations or performs migrations when the 90th percentile I/O latency measured over a day for the datastore is greater than the threshold.

You can also set advanced options to further configure the aggressiveness level of Storage DRS.

Space utilization difference	This threshold ensures that there is some minimum difference between the space utilization of the source and the destination. For example, if the space used on datastore A is 82% and datastore B is 79%, the difference is 3. If the threshold is 5, Storage DRS will not make migration recommendations from datastore A to datastore B.
I/O load balancing invocation interval	After this interval, Storage DRS runs to balance I/O load.
I/O imbalance threshold	Lowering this value makes I/O load balancing less aggressive. Storage DRS computes an I/O fairness metric between 0 and 1, which 1 being the fairest distribution. I/O load balancing runs only if the computed metric is less than 1 - (I/O imbalance threshold / 100).

Set Storage DRS Runtime Rules

Set Storage DRS triggers and configure advanced options for the datastore cluster.

1. Optional: Select or deselect the **Enable I/O metric for SDRS recommendations** check box to activate or deactivate I/O metric inclusion.

   When you deactivate this option, vCenter Server does not consider I/O metrics when making Storage DRS recommendations. When you deactivate this option, you deactivate the following elements of Storage DRS:

   - I/O load balancing among datastores within a datastore cluster.
   - Initial placement for virtual disks based on I/O workload. Initial placement is based on space only.

2. Optional: Set Storage DRS thresholds.

   You set the aggressiveness level of Storage DRS by specifying thresholds for used space and I/O latency.

   - Use the Utilized Space slider to indicate the maximum percentage of consumed space allowed before Storage DRS is triggered. Storage DRS makes recommendations and performs migrations when space use on the datastores is higher than the threshold.
   - Use the I/O Latency slider to indicate the maximum I/O latency allowed before Storage DRS is triggered. Storage DRS makes recommendations and performs migrations when latency is higher than the threshold.

     Note: The Storage DRS I/O Latency threshold for the datastore cluster should be lower than or equal to the Storage I/O Control congestion threshold.

3. Optional: Configure advanced options.

   - No recommendations until utilization difference between source and destination is: Use the slider to specify the space utilization difference threshold. Utilization is usage * 100/capacity.

     This threshold ensures that there is some minimum difference between the space utilization of the source and the destination. For example, if the space used on datastore A is 82% and datastore B is 79%, the difference is 3. If the threshold is 5, Storage DRS will not make migration recommendations from datastore A to datastore B.
   - Check imbalances every: Specify how often Storage DRS should assess space and I/O load balancing.
   - I/O imbalance threshold: Use the slider to indicate the aggressiveness of I/O load balancing. Lowering this value makes I/O load balancing less aggressive. Storage DRS computes an I/O fairness metric between 0 and 1, which 1 being the fairest distribution. I/O load balancing runs only if the computed metric is less than 1 - (I/O imbalance threshold / 100).

4. Click **OK**.

Datastore Cluster Requirements

Datastores and hosts that are associated with a datastore cluster must meet certain requirements to use datastore cluster features successfully.

Follow these guidelines when you create a datastore cluster.

- Datastore clusters must contain similar or interchangeable datastores.
  A datastore cluster can contain a mix of datastores with different sizes and I/O capacities, and can be from different arrays and vendors. However, the following types of datastores cannot coexist in a datastore cluster.
  - NFS and VMFS datastores cannot be combined in the same datastore cluster.
  - Replicated datastores cannot be combined with non-replicated datastores in the same Storage-DRS-enabled datastore cluster.
- All hosts attached to the datastores in a datastore cluster must be ESXi 5.0 and later. If datastores in the datastore cluster are connected to ESX/ESXi 4.x and earlier hosts, Storage DRS does not run.
- Datastores shared across multiple data centers cannot be included in a datastore cluster.
- As a best practice, do not include datastores that have hardware acceleration enabled in the same datastore cluster as datastores that do not have hardware acceleration enabled. Datastores in a datastore cluster must be homogeneous to guarantee hardware acceleration-supported behavior.

Adding and Removing Datastores from a Datastore Cluster

You add and remove datastores to and from an existing datastore cluster.

You can add to a datastore cluster any datastore that is mounted on a host in the vSphere Client inventory, with the following exceptions:

- All hosts attached to the datastore must be ESXi 5.0 and later.
- The datastore cannot be in more than one data center in the same instance of the vSphere Client.

When you remove a datastore from a datastore cluster, the datastore remains in the vSphere Client inventory and is not unmounted from the host.

Using Datastore Clusters to Manage Storage Resources

After you create a datastore cluster, you can customize it and use it to manage storage I/O and space utilization resources.

Using Storage DRS Maintenance Mode

You place a datastore in maintenance mode when you need to take it out of use to service it. A datastore enters or leaves maintenance mode only as the result of a user request.

Maintenance mode is available to datastores within a Storage DRS-enabled datastore cluster. Standalone datastores cannot be placed in maintenance mode.

Virtual disks that are located on a datastore that is entering maintenance mode must be migrated to another datastore, either manually or using Storage DRS. When you attempt to put a datastore in maintenance mode, the **Placement Recommendations** tab displays a list of migration recommendations, datastores within the same datastore cluster where virtual disks can be migrated. On the **Faults** tab, vCenter Server displays a list of the disks that cannot be migrated and the reasons why. If Storage DRS affinity or anti-affinity rules prevent disks from being migrated, you can choose to enable the Ignore Affinity Rules for Maintenance option.

The datastore is in a state of Entering Maintenance Mode until all virtual disks have been migrated.

Place a Datastore in Maintenance Mode

If you need to take a datastore out of service, you can place the datastore in Storage DRS maintenance mode.

Storage DRS is enabled on the datastore cluster that contains the datastore that is entering maintenance mode.

No CD-ROM image files are stored on the datastore.

There are at least two datastores in the datastore cluster.

1. Browse to the datastore in the vSphere Client.
2. Right-click the datastore and select **Maintenance Mode** > **Enter Maintenance Mode**.
   A list of recommendations appears for datastore maintenance mode migration.
3. Optional: On the Placement Recommendations tab, deselect any recommendations you do not want to apply.

   Note: The datastore cannot enter maintenance mode without evacuating all disks. If you deselect recommendations, you must manually move the affected virtual machines.
4. If necessary, click **Apply Recommendations**.
   vCenter Server uses Storage vMotion to migrate the virtual disks from the source datastore to the destination datastore and the datastore enters maintenance mode.

The datastore icon might not be immediately updated to reflect the datastore's current state. To update the icon immediately, click **Refresh**.

Ignore Storage DRS Affinity Rules for Maintenance Mode

Storage DRS affinity or anti-affinity rules might prevent a datastore from entering maintenance mode. You can ignore these rules when you put a datastore in maintenance mode.

When you activate the Ignore Affinity Rules for Maintenance option for a datastore cluster, vCenter Server ignores Storage DRS affinity and anti-affinity rules that prevent a datastore from entering maintenance mode.

Storage DRS rules are ignored only for evacuation recommendations. vCenter Server does not violate the rules when making space and load balancing recommendations or initial placement recommendations.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Select **DRS** and click **Edit**.
4. Expand **Advanced Options** and click **Add**.
5. In the Option column, type `IgnoreAffinityRulesForMaintenance`.
6. In the Value column, type `1` to activate the option.
   Type `0` to deactivate the option.
7. Click **OK**.

The Ignore Affinity Rules for Maintenance Mode option is applied to the datastore cluster.

Applying Storage DRS Recommendations

Storage DRS collects resource usage information for all datastores in a datastore cluster. Storage DRS uses the information to generate recommendations for virtual machine disk placement on datastores in a datastore cluster.

Storage DRS recommendations appear on the **Storage DRS** tab in the vSphere Client datastore view. Recommendations also appear when you attempt to put a datastore into Storage DRS maintenance mode. When you apply Storage DRS recommendations, vCenter Server uses Storage vMotion to migrate virtual machine disks to other datastores in the datastore cluster to balance the resources.

You can apply a subset of the recommendations by selecting the Override Suggested DRS Recommendations check box and selecting each recommendation to apply.

Table 338: Storage DRS Recommendations

Label	Description
Priority	Priority level (1-5) of the recommendation. (Hidden by default.)
Recommendation	Action being recommended by Storage DRS.
Reason	Why the action is needed.
Space Utilization % Before (source) and (destination)	Percentage of space used on the source and destination datastores before migration.
Space Utilization % After (source) and (destination)	Percentage of space used on the source and destination datastores after migration.
I/O Latency Before (source)	Value of I/O latency on the source datastore before migration.
I/O Latency Before (destination)	Value of I/O latency on the destination datastore before migration.

Refresh Storage DRS Recommendations

Storage DRS migration recommendations appear on the **Storage DRS** tab in the vSphere Client. You can refresh these recommendations by running Storage DRS.

At least one datastore cluster must exist in the vSphere Client inventory.

Enable Storage DRS for the datastore cluster. The **Storage DRS** tab appears only if Storage DRS is enabled.

1. In the vSphere Client datastore view, select the datastore cluster and click the **Storage DRS** tab.
2. Select the **Recommendations** view and click the **Run Storage DRS** link in the upper right corner.

The recommendations are updated. The Last Updated timestamp displays the time when Storage DRS recommendations were refreshed.

Change Storage DRS Automation Level for a Virtual Machine

You can override the datastore cluster-wide automation level for individual virtual machines. You can also override default virtual disk affinity rules.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Configuration**.
3. Under **VM Overrides**, select **Add**.
4. Select a virtual machine.
5. Click the Automation level drop-down menu, and select an automation level for the virtual machine.

Option	Description
Default (Manual)	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.
Disabled	vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

6. Click the **Keep VMDKs together**, drop-down menu to override default VMDK affinity.
   See Override VMDK Affinity Rules.

7. Click **OK**.

Set Up Off-Hours Scheduling for Storage DRS

You can create a scheduled task to change Storage DRS settings for a datastore cluster so that migrations for fully automated datastore clusters are more likely to occur during off-peak hours.

Enable Storage DRS.

You can create a scheduled task to change the automation level and aggressiveness level for a datastore cluster. For example, you might configure Storage DRS to run less aggressively during peak hours, when performance is a priority, to minimize the occurrence of storage migrations. During non-peak hours, Storage DRS can run in a more aggressive mode and be invoked more frequently.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Services**.
3. Under **Storage DRS** click the **Schedule DRS** button.
4. In the Edit Datastore Cluster dialog box, click **SDRS Scheduling**.
5. Expand **DRS Automation**.
   a) Select an automation level.
   b) Set the Migration threshold.

      Use the Migration slider to select the priority level of vCenter Server recommendations that adjust the cluster's load balance.
   c) Select whether to enable Virtual Machine Automation.

      Override for individual virtual machines can be set from the VM Overrides page.
6. Expand **Power Managment**.
   a) Select an automation level.
   b) Set the DPM threshold.

      Use the DPM slider to select the power recommendations that vCenter Server will apply.
7. Type a Task name.
8. Type a description of the Task you have created.
9. Under Configured Scheduler, click **Change** and select the time for the task to run and click **OK**.
10. Type an email address to send a notification email to when the task is complete.
11. Click **OK**.

The scheduled task runs at the specified time.

Storage DRS Anti-Affinity Rules

You can create Storage DRS anti-affinity rules to control which virtual disks should not be placed on the same datastore within a datastore cluster. By default, a virtual machine's virtual disks are kept together on the same datastore.

When you create an anti-affinity rule, it applies to the relevant virtual disks in the datastore cluster. Anti-affinity rules are enforced during initial placement and Storage DRS-recommendation migrations, but are not enforced when a migration is initiated by a user.

Note: Anti-affinity rules do not apply to CD-ROM ISO image files that are stored on a datastore in a datastore cluster, nor do they apply to swapfiles that are stored in user-defined locations.

VM Anti-Affinity Rules	Specify which virtual machines should never be kept on the same datastore. See Create VM Anti-Affinity Rules.
VMDK Anti-Affinity Rules	Specify which virtual disks associated with a particular virtual machine must be kept on different datastores. See Create VMDK Anti-Affinity Rules.

If you move a virtual disk out of the datastore cluster, the affinity or anti-affinity rule no longer applies to that disk.

When you move virtual disk files into a datastore cluster that has existing affinity and anti-affinity rules, the following behavior applies:

- Datastore Cluster B has an intra-VM affinity rule. When you move a virtual disk out of Datastore Cluster A and into Datastore Cluster B, any rule that applied to the virtual disk for a given virtual machine in Datastore Cluster A no longer applies. The virtual disk is now subject to the intra-VM affinity rule in Datastore Cluster B.
- Datastore Cluster B has an VM anti-affinity rule. When you move a virtual disk out of Datastore Cluster A and into Datastore Cluster B, any rule that applied to the virtual disk for a given virtual machine in Datastore Cluster A no longer applies. The virtual disk is now subject to the VM anti-affinity rule in Datastore Cluster B.
- Datastore Cluster B has an VMDK anti-affinity rule. When you move a virtual disk out of Datastore Cluster A and into Datastore Cluster B, the VMDK anti-affinity rule does not apply to the virtual disk for a given virtual machine because the rule is limited to only specified virtual disks in Datastore Cluster B.

Note: Storage DRS rules might prevent a datastore from entering maintenance mode. You can choose to ignore Storage DRS rules for maintenance mode by enabling the Ignore Affinity Rules for Maintenance option.

Create VM Anti-Affinity Rules

You can create an anti-affinity rule to indicate that all virtual disks of certain virtual machines must be kept on different datastores. The rule applies to individual datastore clusters.

Virtual machines that participate in an VM anti-affinity rule in a datastore cluster must be associated with an intra-VM affinity rule in the datastore cluster. The virtual machines must also comply with the intra-VM affinity rule.

If a virtual machine is subject to an VM anti-affinity rule, the following behavior applies:

- Storage DRS places the virtual machine's virtual disks according to the rule.
- Storage DRS migrates the virtual disks using vMotion according to the rule, even if the migration is for a mandatory reason such as putting a datastore in maintenance mode.
- If the virtual machine's virtual disk violates the rule, Storage DRS makes migration recommendations to correct the error or reports the violation as a fault if it cannot make a recommendation that will correct the error.

No VM anti-affinity rules are defined by default.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Configuration**.
3. Select **VM/Host Rules**.
4. Click **Add**.
5. Type a name for the rule.
6. From the Type menu, select **VM anti-affinity**.
7. Click **Add**.
8. Click **Select Virtual Machine**.
9. Select at least two virtual machines and click **OK**.
10. Click **OK** to save the rule.

Create VMDK Anti-Affinity Rules

You can create a VMDK anti-affinity rule for a virtual machine that indicates which of its virtual disks must be kept on different datastores.

VMDK anti-affinity rules apply to the virtual machine for which the rule is defined, not to all virtual machines. The rule is expressed as a list of virtual disks that are to be separated from one another.

If you attempt to set an VMDK anti-affinity rule and an intra-VM affinity rule for a virtual machine, vCenter Server rejects the most recently defined rule.

If a virtual machine is subject to a VMDK anti-affinity rule, the following behavior applies:

- Storage DRS places the virtual machine's virtual disks according to the rule.
- Storage DRS migrates the virtual disks using vMotion according to the rule, even if the migration is for a mandatory reason such as putting a datastore in maintenance mode.
- If the virtual machine's virtual disk violates the rule, Storage DRS makes migration recommendations to correct the error or reports the violation as a fault if it cannot make a recommendation that will correct the error.

No VMDK anti-affinity rules are defined by default.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Configuration**.
3. Select **VM/Host Rules**.
4. Click **Add**.
5. Type a name for the rule.
6. From the Type menu, select **VMDK anti-affinity**.
7. Click **Add**.
8. Click **Select Virtual Machine**.
9. Select a virtual machine and click **OK**.
10. Select at least two virtual disks to which the rule applies and click **OK**.
11. Click **OK** to save the rule.

Override VMDK Affinity Rules

VMDK affinity rules indicate that all virtual disks in a datastore cluster that are associated with a particular virtual machine are located on the same datastore in the datastore cluster. The rules apply to individual datastore clusters.

VMDK affinity rules are activated by default for all virtual machines that are in a datastore cluster. You can override the default setting for the datastore cluster or for individual virtual machines.

Virtual machines that are subject to VMDK affinity rules have the following behavior:

- Storage DRS places the virtual machine's virtual disks according to the rule.
- Storage DRS migrates the virtual disks using vMotion according to the rule, even if the migration is for a mandatory reason such as putting a datastore in maintenance mode.
- If the virtual machine's virtual disk violates the rule, Storage DRS makes migration recommendations to correct the error or reports the violation as a fault if it cannot make a recommendation that will correct the error.

When you add a datastore to a datastore cluster that is activated for Storage DRS, the VMDK affinity rule is deactivated for any virtual machine that has virtual disks on that datastore if it also has virtual disks on other datastores.

1. Browse to the datastore cluster in the vSphere Client.
2. Click the **Configure** tab and click **Configuration**.
3. Select **VM Overrides**.
4. Click **Add**.
5. Use the **+** button to select virtual machines.
6. Click the **Keep VMDKs together** drop-down menu and select **No**.
7. Click **OK**.

Clear Storage DRS Statistics

To diagnose problems with Storage DRS, you can clear Storage DRS statistics before you manually run Storage DRS.

Activate Storage DRS for the datastore cluster.

Important: When you activate the option to clear Storage DRS statistics, statistics are cleared every time Storage DRS runs until you deactivate the option. Always deactivate the option after you diagnose the Storage DRS problem.

1. Activate the `ClearIoStatsOnSdrsRun` option.
   a) Browse to the datastore cluster in the vSphere Client.
   b) Click the **Configuration** tab and click **Services**.
   c) Select **vSphere DRS** and click **Edit**.
   d) Expand **Advanced Options** and click **Add**.
   e) In the Option column, type `ClearIoStatsOnSdrsRun`.
   f) In the corresponding Value text box, type `1`.
   g) Click **OK**.
2. Run Storage DRS on the datastore cluster.

   The current Storage DRS statistics for all datastores and virtual disks in all datastore clusters in the vSphere Client inventory are cleared, but no new statistics are collected.
3. Change the `ClearIoStatsOnSdrsRun` flag value to `0` to deactivate it.
4. Run Storage DRS again.

   Storage DRS runs normally. Allow several hours for the new setting to take effect.

Storage vMotion Compatibility with Datastore Clusters

A datastore cluster has certain vSphere Storage vMotion® requirements.

- The host must be running a version of ESXi that supports Storage vMotion.
- The host must have write access to both the source datastore and the destination datastore.
- The host must have enough free memory resources to accommodate Storage vMotion.
- The destination datastore must have sufficient disk space.
- The destination datastore must not be in maintenance mode or entering maintenance mode.

Using NUMA Systems with ESXi

ESXi supports memory access optimization for Intel and AMD Opteron processors in server architectures that support NUMA (non-uniform memory access).

After you understand how ESXi NUMA scheduling is performed and how the VMware NUMA algorithms work, you can specify NUMA controls to optimize the performance of your virtual machines.

What is NUMA?

NUMA systems are advanced server platforms with more than one system bus. They can harness large numbers of processors in a single system image with superior price to performance ratios.

For the past decade, processor clock speed has increased dramatically. A multi-gigahertz CPU, however, needs to be supplied with a large amount of memory bandwidth to use its processing power effectively. Even a single CPU running a memory-intensive workload, such as a scientific computing application, can be constrained by memory bandwidth.

This problem is amplified on symmetric multiprocessing (SMP) systems, where many processors must compete for bandwidth on the same system bus. Some high-end systems often try to solve this problem by building a high-speed data bus. However, such a solution is expensive and limited in scalability.

NUMA is an alternative approach that links several small, cost-effective nodes using a high-performance connection. Each node contains processors and memory, much like a small SMP system. However, an advanced memory controller allows a node to use memory on all other nodes, creating a single system image. When a processor accesses memory that does

not lie within its own node (remote memory), the data must be transferred over the NUMA connection, which is slower than accessing local memory. Memory access times are not uniform and depend on the location of the memory and the node from which it is accessed, as the technology's name implies.

Challenges for Operating Systems

Because a NUMA architecture provides a single system image, it can often run an operating system with no special optimizations.

The high latency of remote memory accesses can leave the processors under-utilized, constantly waiting for data to be transferred to the local node, and the NUMA connection can become a bottleneck for applications with high-memory bandwidth demands.

Furthermore, performance on such a system can be highly variable. It varies, for example, if an application has memory located locally on one benchmarking run, but a subsequent run happens to place all of that memory on a remote node. This phenomenon can make capacity planning difficult.

Some high-end UNIX systems provide support for NUMA optimizations in their compilers and programming libraries. This support requires software developers to tune and recompile their programs for optimal performance. Optimizations for one system are not guaranteed to work well on the next generation of the same system. Other systems have allowed an administrator to explicitly decide on the node on which an application should run. While this might be acceptable for certain applications that demand 100 percent of their memory to be local, it creates an administrative burden and can lead to imbalance between nodes when workloads change.

Ideally, the system software provides transparent NUMA support, so that applications can benefit immediately without modifications. The system should maximize the use of local memory and schedule programs intelligently without requiring constant administrator intervention. Finally, it must respond well to changing conditions without compromising fairness or performance.

How ESXi NUMA Scheduling Works

ESXi uses a sophisticated NUMA scheduler to dynamically balance processor load and memory locality or processor load balance.

1. Each virtual machine managed by the NUMA scheduler is assigned a home node. A home node is one of the system's NUMA nodes containing processors and local memory, as indicated by the System Resource Allocation Table (SRAT).
2. When memory is allocated to a virtual machine, the ESXi host preferentially allocates it from the home node. The virtual CPUs of the virtual machine are constrained to run on the home node to maximize memory locality.
3. The NUMA scheduler can dynamically change a virtual machine's home node to respond to changes in system load. The scheduler might migrate a virtual machine to a new home node to reduce processor load imbalance. Because this might cause more of its memory to be remote, the scheduler might migrate the virtual machine's memory dynamically to its new home node to improve memory locality. The NUMA scheduler might also swap virtual machines between nodes when this improves overall memory locality.

Some virtual machines are not managed by the ESXi NUMA scheduler. For example, if you manually set the processor or memory affinity for a virtual machine, the NUMA scheduler might not be able to manage this virtual machine. Virtual machines that are not managed by the NUMA scheduler still run correctly. However, they don't benefit from ESXi NUMA optimizations.

The NUMA scheduling and memory placement policies in ESXi can manage all virtual machines transparently, so that administrators do not need to address the complexity of balancing virtual machines between nodes explicitly.

The optimizations work seamlessly regardless of the type of guest operating system. ESXi provides NUMA support even to virtual machines that do not support NUMA hardware, such as Windows NT 4.0. As a result, you can take advantage of new hardware even with legacy operating systems.

A virtual machine that has more virtual processors than the number of physical processor cores available on a single hardware node can be managed automatically. The NUMA scheduler accommodates such a virtual machine by having it span NUMA nodes. That is, it is split up as multiple NUMA clients, each of which is assigned to a node and then managed by the scheduler as a normal, non-spanning client. This can improve the performance of certain memory-intensive workloads with high locality. For information on configuring the behavior of this feature, see Advanced Virtual Machine Attributes.

ESXi 5.0 and later includes support for exposing virtual NUMA topology to guest operating systems. For more information about virtual NUMA control, see Using Virtual NUMA.

VMware NUMA Optimization Algorithms and Settings

This section describes the algorithms and settings used by ESXi to maximize application performance while still maintaining resource guarantees.

Home Nodes and Initial Placement

When a virtual machine is powered on, ESXi assigns it a home node. A virtual machine runs only on processors within its home node, and its newly allocated memory comes from the home node as well.

Unless a virtual machine's home node changes, it uses only local memory, avoiding the performance penalties associated with remote memory accesses to other NUMA nodes.

When a virtual machine is powered on, it is assigned an initial home node so that the overall CPU and memory load among NUMA nodes remains balanced. Because internode latencies in a large NUMA system can vary greatly, ESXi determines these internode latencies at boot time and uses this information when initially placing virtual machines that are wider than a single NUMA node. These wide virtual machines are placed on NUMA nodes that are close to each other for lowest memory access latencies.

Initial placement-only approaches are usually sufficient for systems that run only a single workload, such as a benchmarking configuration that remains unchanged as long as the system is running. However, this approach is unable to guarantee good performance and fairness for a datacenter-class system that supports changing workloads. Therefore, in addition to initial placement, ESXi 5.0 does dynamic migration of virtual CPUs and memory between NUMA nodes for improving CPU balance and increasing memory locality.

Dynamic Load Balancing and Page Migration

ESXi combines the traditional initial placement approach with a dynamic rebalancing algorithm. Periodically (every two seconds by default), the system examines the loads of the various nodes and determines if it should rebalance the load by moving a virtual machine from one node to another.

This calculation takes into account the resource settings for virtual machines and resource pools to improve performance without violating fairness or resource entitlements.

The rebalancer selects an appropriate virtual machine and changes its home node to the least loaded node. When it can, the rebalancer moves a virtual machine that already has some memory located on the destination node. From that point on (unless it is moved again), the virtual machine allocates memory on its new home node and it runs only on processors within the new home node.

Rebalancing is an effective solution to maintain fairness and ensure that all nodes are fully used. The rebalancer might need to move a virtual machine to a node on which it has allocated little or no memory. In this case, the virtual machine incurs a performance penalty associated with a large number of remote memory accesses. ESXi can eliminate this penalty by transparently migrating memory from the virtual machine's original node to its new home node:

1. The system selects a page (4KB of contiguous memory) on the original node and copies its data to a page in the destination node.

2. The system uses the virtual machine monitor layer and the processor's memory management hardware to seamlessly remap the virtual machine's view of memory, so that it uses the page on the destination node for all further references, eliminating the penalty of remote memory access.

When a virtual machine moves to a new node, the ESXi host immediately begins to migrate its memory in this fashion. It manages the rate to avoid overtaxing the system, particularly when the virtual machine has little remote memory remaining or when the destination node has little free memory available. The memory migration algorithm also ensures that the ESXi host does not move memory needlessly if a virtual machine is moved to a new node for only a short period.

When initial placement, dynamic rebalancing, and intelligent memory migration work in conjunction, they ensure good memory performance on NUMA systems, even in the presence of changing workloads. When a major workload change occurs, for instance when new virtual machines are started, the system takes time to readjust, migrating virtual machines and memory to new locations. After a short period, typically seconds or minutes, the system completes its readjustments and reaches a steady state.

Transparent Page Sharing Optimized for NUMA

Many ESXi workloads present opportunities for sharing memory across virtual machines.

For example, several virtual machines might be running instances of the same guest operating system, have the same applications or components loaded, or contain common data. In such cases, ESXi systems use a proprietary transparent page-sharing technique to securely eliminate redundant copies of memory pages. With memory sharing, a workload running in virtual machines often consumes less memory than it would when running on physical machines. As a result, higher levels of overcommitment can be supported efficiently.

Transparent page sharing for ESXi systems has also been optimized for use on NUMA systems. On NUMA systems, pages are shared per-node, so each NUMA node has its own local copy of heavily shared pages. When virtual machines use shared pages, they don't need to access remote memory.

Note: This default behavior is the same in all previous versions of ESX and ESXi.

Resource Management in NUMA Architectures

You can perform resource management with different types of NUMA architecture.

With the proliferation of highly multicore systems, NUMA architectures are becoming more popular as these architectures allow better performance scaling of memory intensive workloads. All modern Intel and AMD systems have NUMA support built into the processors. Additionally, there are traditional NUMA systems like the IBM Enterprise X-Architecture that extend Intel and AMD processors with NUMA behavior with specialized chipset support.

Typically, you can use BIOS settings to activate and deactivate NUMA behavior. For example, in AMD Opteron-based HP Proliant servers, NUMA can be deactivated by activating node interleaving in the BIOS. If NUMA is activated, the BIOS builds a system resource allocation table (SRAT) which ESXi uses to generate the NUMA information used in optimizations. For scheduling fairness, NUMA optimizations are not activated for systems with too few cores per NUMA node or too few cores overall. You can modify the `numa.rebalancecorestotal` and `numa.rebalancecoresnode` options to change this behavior.

Using Virtual NUMA

vSphere includes support for exposing virtual NUMA topology to guest operating systems, which can improve performance by facilitating guest operating system and application NUMA optimizations.

Virtual NUMA topology is available to hardware version 8 virtual machines and is activated by default when the number of virtual CPUs is greater than eight. You can also manually influence virtual NUMA topology using advanced configuration options.

The first time a virtual NUMA activated virtual machine is powered on, its virtual NUMA topology is based on the NUMA topology of the underlying physical host. Once a virtual machines virtual NUMA topology is initialized, it does not change unless the number of vCPUs in that virtual machine is changed.

The virtual NUMA topology does not consider the memory configured to a virtual machine. The virtual NUMA topology is not influenced by the number of virtual sockets and number of cores per socket for a virtual machine.

If the virtual NUMA topology needs to be overridden, see Virtual NUMA Controls.

Note: Activating CPU HotAdd will deactivate virtual NUMA. See https://kb.vmware.com/kb/2040375.

Virtual NUMA Controls

For virtual machines with disproportionately large memory consumption, you can use advanced options to override the default virtual CPU settings.

You can add these advanced options to the virtual machine configuration file.

Table 339: Advanced Options for Virtual NUMA Controls

Option	Description	Default Value
`cpuid.coresPerSocket`	Determines the number of virtual cores per virtual CPU socket. This option does not affect the virtual NUMA topology unless numa.vcpu.followcorespersocket is configured.	1
`numa.vcpu.maxPerVirtualNode`	Determines the number of virtual NUMA nodes by splitting the total vCPU count evenly with this value as its divisor.	8
`numa.autosize.once`	When you create a virtual machine template with these settings, the settings remain the same every time you then power on the virtual machine with the default value TRUE. If the value is set to FALSE, the virtual NUMA topology is updated every time it is powered on. The virtual NUMA topology is reevaluated when the configured number of virtual CPUs on the virtual machine is modified at any time.	TRUE
`numa.vcpu.min`	The minimum number of virtual CPUs in a virtual machine that are required to generate a virtual NUMA topology. A virtual machine is always UMA when its size is smaller than numa.vcpu.min	9
`numa.vcpu.followcorespersocket`	If set to 1, reverts to the old behavior of virtual NUMA node sizing being tied to cpuid.coresPerSocket.	0

Specifying NUMA Controls

If you have applications that use a lot of memory or have a small number of virtual machines, you might want to optimize performance by specifying virtual machine CPU and memory placement explicitly.

Specifying controls is useful if a virtual machine runs a memory-intensive workload, such as an in-memory database or a scientific computing application with a large data set. You might also want to optimize NUMA placements manually if the system workload is known to be simple and unchanging. For example, an eight-processor system running eight virtual machines with similar workloads is easy to optimize explicitly.

Note: In most situations, the ESXi host's automatic NUMA optimizations result in good performance.

ESXi provides three sets of controls for NUMA placement, so that administrators can control memory and processor placement of a virtual machine.

You can specify the following options.

NUMA Node Affinity	When you set this option, NUMA can schedule a virtual machine only on the nodes specified in the affinity.
CPU Affinity	When you set this option, a virtual machine uses only the processors specified in the affinity.
Memory Affinity	When you set this option, the server allocates memory only on the specified nodes.

A virtual machine is still managed by NUMA when you specify NUMA node affinity, but its virtual CPUs can be scheduled only on the nodes specified in the NUMA node affinity. Likewise, memory can be obtained only from the nodes specified in the NUMA node affinity. When you specify CPU or memory affinities, a virtual machine ceases to be managed by NUMA. NUMA management of these virtual machines is effective when you remove the CPU and memory affinity constraints.

Manual NUMA placement might interfere with ESXi resource management algorithms, which distribute processor resources fairly across a system. For example, if you manually place 10 virtual machines with processor-intensive workloads on one node, and manually place only 2 virtual machines on another node, it is impossible for the system to give all 12 virtual machines equal shares of systems resources.

Associate Virtual Machines with Specific Processors

You might be able to improve the performance of the applications on a virtual machine by pinning its virtual CPUs to fixed processors. This allows you to prevent the virtual CPUs from migrating across NUMA nodes.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select the **Virtual Hardware** tab, and expand **CPU**.
4. Under Scheduling Affinity, set the CPU affinity to the preferred processors.

   Note: You must manually select all processors in the NUMA node. CPU affinity is specified on a per-processor, not on a per-node, basis.

Associate Memory Allocations with Specific NUMA Nodes Using Memory Affinity

You can specify that all future memory allocations on a virtual machine use pages associated with specific NUMA nodes (also known as manual memory affinity).

Note: Specify nodes to be used for future memory allocations only if you have also specified CPU affinity. If you make manual changes only to the memory affinity settings, automatic NUMA rebalancing does not work properly.

1. Browse to the virtual machine in the vSphere Client.
2. Click the **Configure** tab.
3. Click **Settings**, and click **VM Hardware**.
4. Click **Edit**.
5. Select the **Virtual Hardware** tab, and expand **Memory**.
6. Under NUMA Memory Affinity, set memory affinity.

   Binding a Virtual Machine to a Single NUMA Node

   The following example illustrates manually binding the last four physical CPUs to a single NUMA node for a two-way virtual machine on an eight-way server.

The CPUs (for example, 4, 5, 6, and 7) are the physical CPU numbers.

1. In the vSphere Client, right-click the virtual machine and select **Edit Settings**.
2. Select **Options** and click **Advanced**.
3. Click the **Configuration Parameters** button.
4. In the vSphere Client, turn on CPU affinity for processors 4, 5, 6, and 7.

Then, you want this virtual machine to run only on node 1.

1. In the vSphere Client inventory panel, select the virtual machine and select **Edit Settings**.
2. Select **Options** and click **Advanced**.
3. Click the **Configuration Parameters** button.
4. In the vSphere Client, set memory affinity for the NUMA node to 1.

Completing these two tasks ensures that the virtual machine runs only on NUMA node 1 and, when possible, allocates memory from the same node.

Associate Virtual Machines with Specified NUMA Nodes

When you associate a NUMA node with a virtual machine to specify NUMA node affinity, you constrain the set of NUMA nodes on which ESXi can schedule a virtual machine's virtual CPU and memory.

Note: When you constrain NUMA node affinities, you might interfere with the ability of the ESXi NUMA scheduler to rebalance virtual machines across NUMA nodes for fairness. Specify NUMA node affinity only after you consider the rebalancing issues.

1. Browse to the VM in the vSphere Client.
2. Right-click and select **Edit Settings**.
3. Select the **VM Options** tab and expand **Advanced**.
4. Under **Configuration Parameters**, click the **Edit Configuration** button.
5. Click **Add Row** to add a new option.
6.
   - To specify NUMA node for the virtual machine, in the Name column, enter `numa.nodeAffinity`.
   - To specify NUMA node for a specific Virtual NUMA node on the virtual machine, in the Name column, enter `sched.nodeX.affinity`, where X is the Virtual NUMA node number. For example, `sched.node0.affinity` specifies Virtual NUMA node 0 on the virtual machine.
7. In the Value column, enter the NUMA nodes where the virtual machine or the virtual NUMA node can be scheduled.

   Use a comma-separated list for multiple nodes. For example, enter `0,1` to constrain the virtual machine resource scheduling to NUMA nodes 0 and 1.
8. Click **OK**.
9. Click **OK** to close the Edit Settings dialog box.

Advanced Attributes

You can set advanced attributes for hosts or individual virtual machines to help you customize resource management.

In most cases, adjusting the basic resource allocation settings (reservation, limit, shares) or accepting default settings results in appropriate resource allocation. However, you can use advanced attributes to customize resource management for a host or a specific virtual machine.

Set Advanced Host Attributes

You can set advanced attributes for a host.

CAUTION: Changing advanced options is considered unsupported. Typically, the default settings produce the optimum result. Change the advanced options only when you get specific instructions from VMware technical support or a knowledge base article.

1. Browse to the host in the vSphere Client.
2. Click the **Configure** tab.
3. Under **System**, click **Advanced System Settings**.
4. Click the **Edit** button.
5. Find the appropriate item and change the value.
6. Click **OK**.

Advanced Memory Attributes

You can use the advanced memory attributes to customize memory resource usage.

Table 340: Advanced Memory Attributes

Attribute	Description	Default
Mem.ShareForceSalting	Mem.ShareForceSalting 0: Inter-virtual machine Transparent Page Sharing (TPS) behavior is still retained. The value of VMX option `sched.mem.pshare.salt` is ignored even if present. Mem.ShareForceSalting 1: By default the salt value is taken from `sched.mem.pshare.salt`. If not specified, it falls back to old TPS (inter-VM) behavior by considering salt values for the virtual machine as 0. Mem.ShareForceSalting 2: By default the salt value is taken from `sched.mem.pshare.salt` if present, or `vc.uuid`. If it does not exist, then the page sharing algorithm generates random and unique value for salting per virtual machine, which is not configurable by users.	2
Mem.SamplePeriod	Specifies the periodic time interval, measured in seconds of the virtual machine's execution time, over which memory activity is monitored to estimate working set sizes.	60
Mem.BalancePeriod	Specifies the periodic time interval, in seconds, for automatic memory reallocations. Significant changes in the amount of free memory also trigger reallocations.	15
Mem.IdleTax	Specifies the idle memory tax rate, as a percentage. This tax effectively charges virtual machines more for idle memory than for memory they are actively using. A tax rate of 0 percent defines an allocation policy that ignores working sets and allocates memory strictly based on shares. A high tax rate results in an allocation policy that allows idle memory to be reallocated away from virtual machines that are unproductively hoarding it.	75
Mem.ShareScanGHz	Specifies the maximum amount of memory pages to scan (per second) for page sharing opportunities for each GHz of available host CPU resource. For example, defaults to 4 MB/sec per 1 GHz.	4
Mem.ShareScanTime	Specifies the time, in minutes, within which an entire virtual machine is scanned for page sharing opportunities. Defaults to 60 minutes.	60

Attribute	Description	Default
Mem.CtlMaxPercent	Limits the maximum amount of memory reclaimed from any virtual machine using the memory balloon driver (`vmmemctl`), based on a percentage of its configured memory size. Specify 0 to deactivate reclamation for all virtual machines.	65
Mem.AllocGuestLargePage	Activates backing of guest large pages with host large pages. Reduces TLB misses and improves performance in server workloads that use guest large pages. 0=deactivate.	1
Mem.AllocUsePSharePool and Mem.AllocUseGuestPool	Reduces memory fragmentation by improving the probability of backing guest large pages with host large pages. If host memory is fragmented, the availability of host large pages is reduced. 0 = deactivate.	15
Mem.MemZipEnable	Activates memory compression for the host. 0 = deactivate.	1
Mem.MemZipMaxPct	Specifies the maximum size of the compression cache in terms of the maximum percentage of each virtual machine's memory that can be stored as compressed memory.	10
LPage.LPageDefragEnable	Activates large page defragmentation. 0 = deactivate.	1
LPage.LPageDefragRateVM	Maximum number of large page defragmentation attempts per second per virtual machine. Accepted values range from 1 to 1024.	32
LPage.LPageDefragRateTotal	Maximum number of large page defragmentation attempts per second. Accepted values range from 1 to 10240.	256
LPage.LPageAlwaysTryForNPT	Try to allocate large pages for nested page tables (called 'RVI' by AMD or 'EPT' by Intel). If you activate this option, all guest memory is backed with large pages in machines that use nested page tables (for example, AMD Barcelona). If NPT is not available, only some portion of guest memory is backed with large pages. 0= deactivate.	1

Advanced NUMA Attributes

You can use the advanced NUMA attributes to customize NUMA usage.

Table 341: Advanced NUMA Attributes

Attribute	Description	Default
Numa.RebalancePeriod	Controls the frequency of rebalance periods, specified in milliseconds. More frequent rebalancing can increase CPU overheads, particularly on machines with a large number of running virtual machines. More frequent rebalancing can also improve fairness.	2000
Numa.MigImbalanceThreshold	The NUMA rebalancer computes the CPU imbalance between nodes, accounting for the difference between each virtual machine’s CPU time entitlement and its actual consumption. This option controls the minimum load imbalance between nodes needed to trigger a virtual machine migration, in percent.	10
Numa.RebalanceEnable	Activate NUMA rebalancing and scheduling. Set this option to 0 to deactivate all NUMA rebalancing and initial placement of virtual machines, effectively deactivating the NUMA scheduling system.	1

Attribute	Description	Default
Numa.RebalanceCoresTotal	Specifies the minimum number of total processor cores on the host required to activate the NUMA rebalancer.	4
Numa.RebalanceCoresNode	Specifies the minimum number of processor cores per node required to activate the NUMA rebalancer. This option and Numa.RebalanceCoresTotal are useful when deactivating NUMA rebalancing on small NUMA configurations (for example, two-way Opteron hosts), where the small number of total or per-node processors can compromise scheduling fairness when you activate NUMA rebalancing.	2
Numa.AutoMemAffinity	Automatically set memory affinity for virtual machines that have CPU affinity set.	1
Numa.PageMigEnable	Automatically migrate pages between NUMA nodes to improve memory locality. Page migration rates set manually are still in effect.	1

Set Advanced Virtual Machine Attributes

You can set advanced attributes for a virtual machine.

Power off the VM before setting advanced attributes.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and select **Edit Settings**.
3. Click **VM Options**.
4. Expand **Advanced**.
5. Under Configuration Parameters, click the **Edit Configuration** button.
6. In the dialog box that appears, click **Add Row** to enter a new parameter and its value.
7. Click **OK**.

Advanced Virtual Machine Attributes

You can use the advanced virtual machine attributes to customize virtual machine configuration.

Table 342: Advanced Virtual Machine Attributes

Attribute	Description	Default
sched.mem.maxmemctl	Maximum amount of memory reclaimed from the selected virtual machine by ballooning, in megabytes (MB). If the ESXi host needs to reclaim additional memory, it is forced to swap. Swapping is less desirable than ballooning.	-1 (Unlimited)
sched.mem.pshare.enable	Enables memory sharing for a selected virtual machine.	True

Attribute	Description	Default
	This boolean value defaults to True. If you set it to False for a virtual machine, this turns off memory sharing.	
sched.mem.pshare.salt	A salt value is a configurable VMX option for each virtual machine. If this option is not present in the virtual machine's VMX file, then the value of `vc.uuid vmx` option is taken as the default value. Since the `vc.uuid` is unique to each virtual machine, by default transparent page sharing happens only among the pages belonging to a particular virtual machine (intra-VM). If a group of virtual machines are considered trustworthy, it is possible to share pages among them by setting a common salt value for all of those virtual machines (inter-VM).	user configurable
sched.swap.persist	Specifies whether the virtual machine's swap files should persist or be deleted when the virtual machine is powered off. By default, the system creates the swap file for a virtual machine when the virtual machine is powered on, and deletes the swap file when the virtual machine is powered off.	False
sched.swap.dir	Directory location of the virtual machine's swap file. Defaults to the virtual machine's working directory, that is, the directory that contains its configuration file. This directory must remain on a host that is accessible to the virtual machine. If you move the virtual machine (or any clones created from it), you might need to reset this attribute.	Equals `workingDir`

Advanced Virtual NUMA Attributes

You can use the advanced virtual NUMA attributes to customize virtual NUMA usage.

Table 343: Advanced NUMA Attributes

Attribute	Description	Default
cpuid.coresPerSocket	Determines the number of virtual cores per virtual CPU socket. If the value is greater than 1, also determines the size of virtual NUMA nodes if a virtual machine has a virtual NUMA topology. You can set this option if you know the exact virtual NUMA topology for each physical host.	1
numa.autosize	When you set this option, the virtual NUMA topology has the same number of virtual CPUs per virtual node as there are cores on each physical node.	FALSE

Attribute	Description	Default
numa.autosize.once	When you create a virtual machine template with these settings, the settings are guaranteed to remain the same every time you subsequently power on the virtual machine. The virtual NUMA topology will be reevaluated if the configured number of virtual CPUs on the virtual machine is modified.	TRUE
numa.vcpu.maxPerVirtualNode	If `cpuid.coresPerSocket` is too restrictive as a power of two, you can set `numa.vcpu.maxPerVirtualNode` directly. In this case, do not set `cpuid.coresPerSocket`.	8
numa.vcpu.min	Minimum number of virtual CPUs in a virtual machine that are required in order to generate a virtual NUMA topology.	9
numa.vcpu.maxPerMachineNode	Maximum number of virtual CPUs that belong to the same virtual machine that can be scheduled on a NUMA node at the same time. Use this attribute to ensure maximum bandwidth, by forcing different NUMA clients on different NUMA nodes.	Number of cores per node on the physical host where a virtual machine is running.
numa.vcpu.maxPerClient	Maximum number of virtual CPUs in a NUMA client. A client is a group of virtual CPUs that are NUMA-managed as a single entity. By default, each virtual NUMA node is a NUMA client, but if a virtual NUMA node is larger than a physical NUMA node, a single virtual NUMA node can be backed by multiple NUMA clients.	Equals `numa.vcpu.maxPerMachineNode`
numa.nodeAffinity	Constrains the set of NUMA nodes on which a virtual machine's virtual CPU and memory can be scheduled. **Note:** When you constrain NUMA node affinities, you might interfere with the ability of the NUMA scheduler to rebalance virtual machines across NUMA nodes for fairness. Specify NUMA node affinity only after you consider the rebalancing issues.	
numa.mem.interleave	Specifies whether the memory allocated to a virtual machine is statically interleaved across all the NUMA nodes on which its constituent NUMA clients are running and there is no virtual NUMA topology exposed.	True

Latency Sensitivity

You can adjust the latency sensitivity of a virtual machine to optimize the scheduling delay for latency sensitive applications.

ESXi is optimized to deliver high throughput. You can optimize your virtual machine to meet the low latency requirement of latency sensitive applications. Examples of latency sensitive applications are VOIP or media player applications, or applications that require frequent access to the mouse or keyboard devices.

Adjust Latency Sensitivity

You can adjust the latency sensitivity of a virtual machine.

ESXi 6.7 requires full CPU reservation to power on a VM with hardware version 14 when Latency Sensitivity is set to **high**.

1. Browse to the virtual machine in the vSphere Client.
   a) To find a virtual machine, select a data center, folder, cluster, resource pool, or host.
   b) Click the **VMs** tab.
2. Right-click the virtual machine and click **Edit Settings**.
3. Click **VM Options** and click **Advanced**.
4. Select a setting from the **Latency Sensitivity** drop-down menu.
5. Click **OK**.

About Reliable Memory

ESXi supports reliable memory.

Some systems have reliable memory, which is a part of memory that is less likely to have hardware memory errors than other parts of the memory in the system. If the hardware exposes information about the different levels of reliability, ESXi might be able to achieve higher system reliability.

View Reliable Memory

You can view whether or not the license permits reliable memory.

1. Browse to the host in the vSphere Client.
2. Click the **Configure** tab and click **System**.
3. Select **Licensing**.
4. Under **Licensed Features** verify Reliable Memory is displayed.

You can look up how much memory is considered reliable by using the ESXCLI `hardware memory get` command.

Backing Guest vRAM with 1GB Pages

vSphere 6.7 ESXi provides a limited support for backing guest vRAM with 1GB pages.

In order to use 1GB pages for backing guest memory you must apply the option `sched.mem.lpage.enable1GPage = "TRUE"` for the VM. You can set this under Advanced options when you select **Edit Settings**. You can only enable 1GB pages on a VM that is powered off.

A VM with 1GB pages enabled must have full memory reservation. Otherwise, the VM will not be able to power on. All of the vRAM for VMs with 1GB pages enabled is preallocated on power-on. Since these VMs have full memory reservation they are not affected by memory reclamation and their memory consumption stays at the maximum level for the entire lifetime of the VM.

1GB page vRAM backing is opportunistic and 1GB pages are allocated on a best effort basis. This includes cases where host CPUs do not have 1GB capabilities. To maximize the chances of having guest vRAM backed with 1GB pages, we recommended to start VMs requiring 1GB pages on a freshly booted host because over time the host RAM is fragmented.

A VM with 1GB pages enabled can be migrated to a different host. However, the 1GB page size might not be allocated on the destination host in the same amount as it was on the source host. You might also see part of vRAM backed with a 1GB page on the source host is no longer backed with a 1GB page on the destination host.

The opportunistic nature of 1GB pages extends to vSphere services such as HA and DRS that might not preserve 1GB page vRAM backing. These services are not aware of 1GB capabilities of destination host and do not take 1GB memory backing into account while making placement decisions.

Fault Definitions

DRS faults indicate the reasons that prevent the generation of DRS actions (or the recommendation of those actions in manual mode).

The DRS faults are defined within this section.

Note: In this chapter, "Memory" can refer to physical RAM or Persistent Memory.

Virtual Machine is Pinned

This fault occurs when DRS cannot move a virtual machine because DRS is deactivated on it. That is, the virtual machine is "pinned" on its registered host.

Virtual Machine not Compatible with any Host

This fault occurs when DRS cannot find a host that can run the virtual machine.

This might occur, for example, if no host can satisfy the virtual machine's CPU or memory resource needs or if no host currently has network or storage access needed by the virtual machine.

To address this problem, provide a host that can meet the virtual machine's requirements.

VM/VM DRS Rule Violated when Moving to another Host

This fault occurs when more than one virtual machines running on the same host and share affinity rules with each other cannot be moved to another host.

This might occur because not all the virtual machines can vMotion off the current host. For example, one of the virtual machines in the group is DRS-deactivated.

To prevent this, check for reasons why some virtual machines in the group cannot vMotion.

Host Incompatible with Virtual Machine

This fault occurs when DRS considers migrating a virtual machine to a host, but finds that the host is incompatible with the given virtual machine.

This might occur because the target host does not have access to the network or storage connection needed by the virtual machine. Another reason this fault occurs is if the target host has a CPU that differs sufficiently from the current host so that using vMotion amongst the hosts is not supported.

To avoid this, create clusters such that all hosts are configured consistently and vMotion is compatible amongst the hosts.

Another reason the host is incompatible with the virtual machine is that there is a required VM/Host DRS rule in place that instructs DRS to never place this virtual machine on this host.

Host Has Virtual Machine That Violates VM/VM DRS Rules

This fault occurs when the virtual machine, when powered on or moved by starting vMotion, might violate a VM/VM DRS rule.

The virtual machine can still be manually powered on or moved with vMotion, but vCenter Server cannot automatically do so.

Host has Insufficient Capacity for Virtual Machine

This fault occurs when the host does not have enough CPU or memory capacity for running the virtual machine.

Host in Incorrect State

This fault occurs when the host is entering maintenance or standby state when needed for DRS action to occur.

To address this fault, cancel the request for the host to enter standby or maintenance mode.

Host Has Insufficient Number of Physical CPUs for Virtual Machine

This fault occurs when the host hardware does not enough CPUs (hyperthreads) to support the number of virtual CPUs in the virtual machine.

Host has Insufficient Capacity for Each Virtual Machine CPU

This fault occurs when the host does not have enough CPU capacity for running the virtual machine.

The Virtual Machine Is in vMotion

This fault occurs when DRS cannot move a virtual machine because it is in vMotion.

No Active Host in Cluster

This fault occurs when the cluster in which the virtual machine is being moved does not contain any hosts that are connected and in a non-maintenance state.

This can occur, for example, when all the hosts are disconnected or in maintenance mode.

Insufficient Resources

This fault occurs when an attempted operation conflicts with a resource configuration policy.

This fault may occur, for example, if a power-on operation reserves more memory than is allocated to a resource pool.

Retry the operation after adjusting the resources to allow more memory.

Insufficient Resources to Satisfy Configured Failover Level for HA

This fault occurs when the HA configuration of CPU or memory resources reserved for failover is violated or is insufficient for the DRS operation.

This fault is reported when:

- The host is requested to enter maintenance or standby mode.
- The virtual machine violates failover when it attempts to power on.

No Compatible Hard Affinity Host

No host is available for the virtual machine that satisfies its mandatory VM/Host DRS affinity or anti-affinity rules.

No Compatible Soft Affinity Host

No host is available for the virtual machine that satisfied its preferred VM/Host DRS affinity or anti-affinity rules.

Soft Rule Violation Correction Disallowed

DRS migration threshold is set at mandatory-only.

This does not allow the generation of DRS actions to correct non-mandatory VM/Host DRS affinity rules.

Soft Rule Violation Correction Impact

Correcting the non-mandatory VM/Host DRS affinity rule does not occur because it impacts performance.

DRS Troubleshooting Information

This information describes vSphere® Distributed Resource Scheduler (DRS) problems for particular categories: cluster, host, and virtual machine problems.

Note: In this chapter, "Memory" can refer to physical RAM or Persistent Memory.

Cluster Problems

Cluster problems can prevent DRS from performing optimally or from reporting faults.

Load Imbalance on Cluster

A cluster has a load imbalance of resources.

A cluster might become unbalanced because of uneven resource demands from virtual machines and unequal capacities of hosts.

The following are possible reasons why the cluster has a load imbalance:

- The migration threshold is too high.
  A higher threshold makes the cluster a more likely candidate for load imbalance.
- VM/VM or VM/Host DRS rules prevent virtual machines from being moved.
- DRS is deactivated for one or more virtual machines.
- A device is mounted to one or more virtual machines preventing DRS from moving the virtual machine in order to balance the load.
- Virtual machines are not compatible with the hosts to which DRS would move them. That is, at least one of the hosts in the cluster is incompatible for the virtual machines that would be migrated. For example, if host A's CPU is not vMotion-compatible with host B's CPU, then host A becomes incompatible for powered-on virtual machines running on host B.
- It would be more detrimental for the virtual machine's performance to move it than for it to run where it is currently located. This may occur when loads are unstable or the migration cost is high compared to the benefit gained from moving the virtual machine.
- vMotion is not activated or set up for the hosts in the cluster.

Address the problem that is causing the load imbalance.

Cluster is Yellow

The cluster is yellow due to a shortage of resources.

If the cluster does not have enough resources to satisfy the reservations of all resource pools and virtual machines, but does have enough resources to satisfy the reservations of all running virtual machines, DRS continues to run and the cluster is yellow.

A cluster can become yellow if the host resources are removed from the cluster (for example, if a host fails).

Add host resources to the cluster or reduce the resource pool reservations.

Cluster is Red Because of Inconsistent Resource Pool

A DRS cluster becomes red when it is invalid. It may become red because the resource pool tree is not internally consistent.

If the cluster resource pool tree is not internally consistent (for example, the sum of the children's reservations is greater than the parent pool's nonexpandable reservation), the cluster does not have enough resources to satisfy the reservations of all running virtual machines making the cluster red.

This can occur if vCenter Server is unavailable or if resource pool settings are changed while a virtual machine is in a failover state.

Revert the associated changes or otherwise revise the resource pool settings.

Cluster Is Red Because Failover Capacity Is Violated

A DRS cluster becomes red when it is invalid. It may become red because failover capacity is violated.

The cluster attempts to fail over virtual machines if there is host failure, but is not guaranteed to have enough resources available to fail over all virtual machines covered by the failover requirements.

If a cluster enabled for HA loses so many resources that it can no longer fulfill its failover requirements, a message appears and the cluster's status changes to red.

Review the list of configuration issues in the yellow box at the top of the cluster Summary page and address the issue that is causing the problem.

No Hosts are Powered Off When Total Cluster Load is Low

Hosts are not powered off when the total cluster load is low.

Hosts are not powered off when the total cluster load is low because extra capacity is needed for HA failover reservations.

Hosts might not be powered off for the following reasons:

- The `MinPoweredOn{Cpu|Memory}Capacity` advanced options settings need to be met.
- Virtual machines cannot be consolidated onto fewer hosts due to their resource reservations, VM/Host DRS rules, VM/VM DRS rules, not being DRS-activated, or not being compatible with the hosts having available capacity.
- Loads are unstable.
- DRS migration threshold is at the highest setting and only allows mandatory moves.
- vMotion is unable to run because it is not configured.
- DPM is deactivated on the hosts that might be powered off.
- Hosts are not compatible for virtual machines to be moved to another host.
- Host does not have Wake On LAN, IPMI, or iLO technology. Either one is required for DPM to enter a host in standby.

Address the issue that prevents hosts from being powered off when the total cluster load is low.

Hosts Are Powered-off When Total Cluster Load Is High

Hosts are powered off when total cluster load is high.

DRS determined that virtual machines can be run on fewer hosts without degrading the host or virtual machine performance. DRS is also constrained from moving the virtual machines running on the highly utilized hosts to the hosts scheduled for power-off.

The total cluster load is too high.

Reduce the cluster load.

DRS Seldom or Never Performs vMotion Migrations

DRS seldom or never performs vMotion migrations.

DRS does not perform vMotion migrations.

DRS never performs vMotion migrations when one or more of the following issues is present on the cluster.

- DRS is deactivated on the cluster.
- The hosts do not have shared storage.
- The hosts in the cluster do not contain a vMotion network.
- DRS is manual and no one has approved the migration.

DRS seldom performs vMotion when one or more of the following issues is present on the cluster:

- Loads are unstable, or vMotion takes a long time, or both. A move is not appropriate.
- DRS seldom or never migrates virtual machines.
- DRS migration threshold is set too high.

DRS moves virtual machines for the following reasons:

- Evacuation of host that a user requested enter maintenance or standby mode.
- VM/Host DRS rules or VM/VM DRS rules.
- Reservation violations.
- Load imbalance.
- Power management.

Address the issues that are causing DRS to avoid performing vMotion migrations.

Host Problems

Host problems might cause DRS to not perform as expected.

DRS Recommends Host Be Powered on to Increase Capacity When Total Cluster Load Is Low

The host must be powered on to help provide more capacity for the cluster or help hosts that are overloaded.

DRS recommends that the host is powered on to increase capacity when the total cluster load is low.

The recommendation might be made because:

- The cluster is a DRS-HA cluster. Additional powered-on hosts are needed to provide more failover capability.
- Some hosts are overloaded and virtual machines on currently powered-on hosts can be moved to hosts in standby mode to balance the load.
- The capacity is necessary to meet the `MinPoweredOn{Cpu|Memory}Capacity` advanced options.

Power on the host.

Total Cluster Load Is High

The total cluster load is high.

When the total cluster load is high, DRS does not power-on the host.

The following are possible reasons why DRS does not power-on the host:

- VM/VM DRS rules or VM/Host DRS rules prevent the virtual machine from being moved to this host.
- Virtual machines are pinned to their current hosts, so DRS cannot move these virtual machines to hosts in standby mode to balance the load.
- DRS or DPM is in manual mode and the recommendations were not applied.
- No virtual machines on highly used hosts are moved to that host.
- DPM is deactivated on the host because of a user setting or host previously failing to exit standby.

Address that issue that prevents DRS from powering on the host.

Total Cluster Load Is Low

The total cluster load is low.

When the total cluster load is low, DRS does not power off the host.

The following are possible reasons why DRS does not power off the host:

- Distributed Power Management (DPM) detected better candidates to power off.
- vSphere HA needs extra capacity for failover.
- The load is not low enough to trigger the host to power off.
- DPM projects that the load will increase.
- DPM is not enabled for the host.
- DPM threshold is set too high.
- While DPM is enabled for the host, no suitable power-on mechanism is present for the host.
- DRS cannot evacuate the host.
- The DRS migration threshold is at the highest setting and only performs mandatory moves.

Address the issue that is preventing DRS from powering off the host.

DRS Does Not Evacuate a Host Requested to Enter Maintenance or Standby Mode

DRS does not evacuate a host requested to enter maintenance mode or standby mode.

When you attempt to put a host into maintenance or standby mode, DRS does not evacuate the host as expected.

vSphere HA is activated and evacuating this host might violate HA failover capacity.

There is no solution. If appropriate, deactivate vSphere HA before you attempt to put the host into maintenance mode or standby mode.

DRS Does Not Move Any Virtual Machines onto a Host

DRS does not move any virtual machines onto a host.

DRS does not recommend migration of virtual machine to a host that has been added to a DRS-activated cluster.

After a host has been added to a DRS-activated cluster, the virtual machines deployed to the host become part of the cluster. DRS can recommend migration of some virtual machines to this host just added to the cluster. If that does not occur, there may be problems with vMotion, host compatibility, or affinity rules. The following are possible reasons:

- vMotion is not configured or activated on this host.
- Virtual machines on other hosts are not compatible with this host.
- The host does not have sufficient resources for any virtual machine.
- Moving any virtual machines to this host would violate a VM/VM DRS rule or VM/Host DRS rule.
- This host is reserved for HA failover capacity.
- A device is mounted to the virtual machine.
- The vMotion threshold is too high.
- DRS is deactivated for the virtual machines, hence the virtual machine could not be moved onto the destination host.

Address the issue that prevents DRS from moving virtual machines onto a host.

DRS Does Not Move Any Virtual Machines from a Host

DRS does not move any virtual machines from a host.

Virtual machines are not moved from this host.

This may be because of problems with vMotion, DRS, or host compatibility. The following are the possible reasons:

- vMotion is not configured or activated on this host.
- DRS is deactivated for the virtual machines on this host.
- Virtual machines on this host are not compatible with any other hosts.
- No other hosts have sufficient resources for any virtual machines on this host.
- Moving any virtual machines from this host would violate a VM/VM DRS rule or VM/Host DRS rule.
- DRS is deactivated for one or more virtual machines on the host.
- A device is mounted to the virtual machine.

Address the issues that are preventing DRS from moving virtual machines from the host.

Virtual Machine Problems

Virtual machine problems might cause DRS to not perform as expected.

Insufficient CPU or Memory Resources

The virtual machine does not receive enough CPU or memory resources.

In some cases, the virtual machine's demand is greater than its resource entitlement. When this occurs, the virtual machine doesn't receive enough CPU or memory resources.

The following sections describe the factors that influence the entitlement for a virtual machine.

Cluster is Yellow or Red	If the cluster is yellow or red, the capacity is insufficient to meet the resource reservations configured for all virtual machines and resource pools in the cluster. The particular virtual machine might be one that is not receiving its reservation. Check the status of the cluster (red or yellow) and resolve the situation.
Resource Limit is Too Restrictive	The virtual machine, its parent resource pool, or its resource pool ancestors might have a configured resource limit that is too restrictive. Check whether demand is equal to or greater than any configured limits.
Cluster is Overloaded	The cluster on which the virtual machine is running might have insufficient resources. Also, the virtual machine's share value is such that other virtual machines are granted proportionally more of the resources. To determine the demand is larger than the capacity, check the cluster statistics.
Host is Overloaded	To determine if the host's resources are oversubscribed, check the host statistics. If they are oversubscribed, consider why DRS is not moving any of the virtual machines now running on the host to other hosts. This condition might exist for the following reasons: • The VM/VM DRS rules and VM/Host DRS rules require the current virtual machine-to-host mapping. If such rules are configured in the cluster, consider deactivating one or more of them. Then run DRS and check whether the situation is corrected.

- DRS cannot move this virtual machine or enough of the other virtual machines to other hosts to free up capacity. DRS will not move a virtual machine for any of the following reasons:
  - DRS is deactivated for the virtual machine.
  - A host device is mounted to the virtual machine.
  - Either of its resource reservations is so large that the virtual machine cannot run on any other host in the cluster.
  - The virtual machine is not compatible with any other host in the cluster.

  Check whether any of these conditions exist for the virtual machine. If none exist, the conditions might exist for other virtual machines in the cluster. If this is the case, DRS cannot balance the cluster to address the virtual machine's demand.
- Decrease the DRS migration threshold setting and check whether the situation is resolved.
- Increase the virtual machine's reservation.

Address the problem that is causing the virtual machine to not receive enough CPU or memory resources.

VM/VM DRS Rule or VM/Host DRS Rule Violated

DRS rules specify which host a virtual machine must or must not reside on, or which virtual machines must be or must not be on the same host.

A VM/VM DRS rule or a VM/Host DRS rule is violated.

VM/VM DRS rules specify that selected virtual machines should be placed on the same host (affinity) or that virtual machines be placed on different hosts (anti-affinity). VM/Host DRS rules specify that selected virtual machines should be placed on specified hosts (affinity) or that selected virtual machines should not be placed on specified hosts (anti-affinity).

When a VM/VM DRS rule or VM/Host DRS rule is violated, it might be because DRS cannot move some or all of the virtual machines in the rule. The reservation of the virtual machine or other virtual machines in the affinity rule, or their parent resource pools, might prevent DRS from locating all virtual machines on the same host.

- Check the DRS faults panel for faults associated with affinity rules.
- Compute the sum of the reservations of all the virtual machines in the affinity rule. If that value is greater than the available capacity on any host, the rule cannot be satisfied.
- Compute the sum of the reservations of their parent resource pools. If that value is greater than the available capacity of any host, the rule cannot be satisfied if the resources are obtained from a single host.

Virtual Machine Power On Operation Fails

An error message appears stating that the virtual machine fails to power on.

The virtual machine fails to power on.

The virtual machine might fail to power on because of insufficient resources or because there are no compatible hosts for the virtual machine.

If the cluster does not have sufficient resources to power on a single virtual machine or any of the virtual machines in a group power-on attempt, check the resources required by the virtual machine against those available in the cluster or its parent resource pool. If necessary, reduce the reservations of the virtual machine to be powered-on, reduce the reservations of its sibling virtual machines, or increase the resources available in the cluster or its parent resource pool.

DRS Does Not Move the Virtual Machine

DRS does not move the virtual machine when it is initially powered on despite insufficient resources on the host.

When you power on a virtual machine, DRS does not migrate it as expected when there are not enough resources on the host where the virtual machine is registered.

The following are possible reasons why DRS does not move the virtual machine.

- DRS is deactivated on the virtual machine.
- The virtual machine has a device mounted.
- The virtual machine is not compatible with any other hosts.
- No other hosts have a sufficient number of physical CPUs or capacity for each CPU for the virtual machine.
- No other hosts have sufficient CPU or memory resources to satisfy the reservations and required memory of this virtual machine.
- Moving the virtual machine will violate an affinity or anti-affinity rule.
- The DRS automation level of the virtual machine is manual and the user does not approve the migration recommendation.
- DRS will not move fault tolerance-activated virtual machines.
- Check if a VM Override definition exists for the VM which may impede an automatic migration.

Address the issue that prevents DRS from moving the virtual machine.

vSphere Availability

vSphere Availability describes solutions that provide business continuity, including how to establish vSphere® High Availability (HA) and vSphere Fault Tolerance.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

This information is for anyone who wants to provide business continuity through the vSphere HA and Fault Tolerance solutions. The information in this book is for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

Business Continuity and Minimizing Downtime

Downtime, whether planned or unplanned, brings considerable costs. However, solutions that ensure higher levels of availability have traditionally been costly, hard to implement, and difficult to manage.

VMware software makes it simpler and less expensive to provide higher levels of availability for important applications. With vSphere, you can increase the baseline level of availability provided for all applications and provide higher levels of availability more easily and cost effectively. With vSphere, you can:

- Provide high availability independent of hardware, operating system, and applications.
- Reduce the planned downtime for common maintenance operations.
- Provide automatic recovery in cases of failure.

vSphere makes it possible to reduce planned downtime, prevent unplanned downtime, and recover rapidly from outages.

Reducing Planned Downtime

Planned downtime typically accounts for over 80% of data center downtime. Hardware maintenance, server migration, and firmware updates all require downtime for physical servers. To minimize the impact of this downtime, organizations are forced to delay maintenance until inconvenient and difficult-to-schedule downtime windows.

vSphere makes it possible for organizations to dramatically reduce planned downtime. Because workloads in a vSphere environment can be dynamically moved to different physical servers without downtime or service interruption, server maintenance can be performed without requiring application and service downtime. With vSphere, organizations can:

- Eliminate downtime for common maintenance operations.
- Eliminate planned maintenance windows.
- Perform maintenance at any time without disrupting users and services.

The vSphere vMotion® and Storage vMotion functionality in vSphere makes it possible for organizations to reduce planned downtime because workloads in a VMware environment can be dynamically moved to different physical servers or to different underlying storage without service interruption. Administrators can perform faster and completely transparent maintenance operations, without being forced to schedule inconvenient maintenance windows.

Preventing Unplanned Downtime

While an ESXi host provides a robust platform for running applications, an organization must also protect itself from unplanned downtime caused from hardware or application failures. vSphere builds important capabilities into data center infrastructure that can help you prevent unplanned downtime.

These vSphere capabilities are part of virtual infrastructure and are transparent to the operating system and applications running in virtual machines. These features can be configured and utilized by all the virtual machines on a physical system, reducing the cost and complexity of providing higher availability. Key availability capabilities are built into vSphere:

- Shared storage. Eliminate single points of failure by storing virtual machine files on shared storage, such as Fibre Channel or iSCSI SAN, or NAS. The use of SAN mirroring and replication features can be used to keep updated copies of virtual disk at disaster recovery sites.
- Network interface teaming. Provide tolerance of individual network card failures.
- Storage multipathing. Tolerate storage path failures.

In addition to these capabilities, the vSphere HA and Fault Tolerance features can minimize or eliminate unplanned downtime by providing rapid recovery from outages and continuous availability, respectively.

vSphere HA Provides Rapid Recovery from Outages

vSphere HA leverages multiple ESXi hosts configured as a cluster to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines.

vSphere HA protects application availability in the following ways:

- It protects against a server failure by restarting the virtual machines on other hosts within the cluster.
- It protects against application failure by continuously monitoring a virtual machine and resetting it in the event that a failure is detected.
- It protects against datastore accessibility failures by restarting affected virtual machines on other hosts which still have access to their datastores.
- It protects virtual machines against network isolation by restarting them if their host becomes isolated on the management or vSAN network. This protection is provided even if the network has become partitioned.

Unlike other clustering solutions, vSphere HA provides the infrastructure to protect all workloads with the infrastructure:

- You do not need to install special software within the application or virtual machine. All workloads are protected by vSphere HA. After vSphere HA is configured, no actions are required to protect new virtual machines. They are automatically protected.
- You can combine vSphere HA with vSphere Distributed Resource Scheduler (DRS) to protect against failures and to provide load balancing across the hosts within a cluster.

vSphere HA has several advantages over traditional failover solutions:

Minimal setup	After a vSphere HA cluster is set up, all virtual machines in the cluster get failover support without additional configuration.
Reduced hardware cost and setup	The virtual machine acts as a portable container for the applications and it can be moved among hosts. Administrators avoid duplicate configurations on multiple machines. When you use vSphere HA, you must have sufficient resources to fail over the number of hosts you want to protect with vSphere HA. However, the VMware vCenter Server® system automatically manages resources and configures clusters.
Increased application availability	Any application running inside a virtual machine has access to increased availability. Because the virtual machine can recover from hardware failure, all applications that start at boot have increased availability without increased computing needs, even if the application is not itself a clustered application. By monitoring and responding to VMware Tools heartbeats and restarting nonresponsive virtual machines, it protects against guest operating system crashes.
DRS and vMotion integration	If a host fails and virtual machines are restarted on other hosts, DRS can provide migration recommendations or migrate virtual machines for balanced resource allocation. If one or both of the

source and destination hosts of a migration fail, vSphere HA can help recover from that failure.

vSphere Fault Tolerance Provides Continuous Availability

vSphere HA provides a base level of protection for your virtual machines by restarting virtual machines in the event of a host failure. vSphere Fault Tolerance provides a higher level of availability, allowing users to protect any virtual machine from a host failure with no loss of data, transactions, or connections.

Fault Tolerance provides continuous availability by ensuring that the states of the Primary and Secondary VMs are identical at any point in the instruction execution of the virtual machine.

If either the host running the Primary VM or the host running the Secondary VM fails, an immediate and transparent failover occurs. The functioning ESXi host seamlessly becomes the Primary VM host without losing network connections or in-progress transactions. With transparent failover, there is no data loss and network connections are maintained. After a transparent failover occurs, a new Secondary VM is respawned and redundancy is re-established. The entire process is transparent and fully automated and occurs even if vCenter Server is unavailable.

Protecting vCenter Server with vCenter High Availability

vCenter High Availability (vCenter HA) protects not only against host and hardware failures but also against vCenter Server application failures. Using automated failover from active to passive, vCenter HA supports high availability with minimal downtime.

You configure vCenter HA from the vSphere Client. The configuration wizard provides these options.

Option	Description
Automatic	The automatic option clones the Active node to the Passive node and witness node, and configures the nodes for you. If your environment meets the following requirements, you can use this option. • The vCenter Server that becomes the Active node is managing its own ESXi host and its own virtual machine. This configuration is sometimes called a self-managed vCenter Server.
Manual	The manual option offers more flexibility. You can use this option provided that your environment meets hardware and software requirements. If you select this option, you are responsible for cloning the Active node to the Passive node and the Witness node. You must also perform some networking configuration.

Protecting vCenter Server with VMware Service Lifecycle Manager

Availability of vCenter Server is provided by VMware Service Lifecycle Manager.

If a vCenter service fails, VMware Service Lifecycle Manager restarts it. VMware Service Lifecycle Manager monitors the health of services and it takes preconfigured remediation action when it detects a failure. Service does not restart if multiple attempts to remediate fail.

Creating and Using vSphere HA Clusters

vSphere HA clusters enable a collection of ESXi hosts to work together so that, as a group, they provide higher levels of availability for virtual machines than each ESXi host can provide individually. When you plan the creation and usage

of a new vSphere HA cluster, the options you select affect the way that cluster responds to failures of hosts or virtual machines.

Before you create a vSphere HA cluster, you should know how vSphere HA identifies host failures and isolation and how it responds to these situations. You also should know how admission control works so that you can choose the policy that fits your failover needs. After you establish a cluster, you can customize its behavior with advanced options and optimize its performance by following recommended best practices.

Note: You might get an error message when you try to use vSphere HA. For information about error messages related to vSphere HA, see the VMware knowledge base article at http://kb.vmware.com/kb/1033634.

How vSphere HA Works

vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

When you create a vSphere HA cluster, a single host is automatically elected as the primary host. The primary host communicates with vCenter Server and monitors the state of all protected virtual machines and of the secondary hosts. Different types of host failures are possible, and the primary host must detect and appropriately deal with the failure. The primary host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The primary host uses network and datastore heartbeating to determine the type of failure.

Primary and Secondary Hosts

When you add a host to a vSphere HA cluster, an agent is uploaded to the host and configured to communicate with other agents in the cluster. Each host in the cluster functions as a primary host or a secondary host.

When vSphere HA is enabled for a cluster, all active hosts (that are not in standby, maintenance mode or not disconnected) participate in an election to choose the cluster's primary host. The host that mounts the greatest number of datastores has an advantage in the election. Only one primary host typically exists per cluster and all other hosts are secondary hosts. If the primary host fails, is shut down or put in standby mode, or is removed from the cluster a new election is held.

The primary host in a cluster has several responsibilities:

- Monitoring the state of secondary hosts. If a secondary host fails or becomes unreachable, the primary host identifies which virtual machines must be restarted.
- Monitoring the power state of all protected virtual machines. If one virtual machine fails, the primary host ensures that it is restarted. Using a local placement engine, the primary host also determines where the restart takes place.
- Managing the lists of cluster hosts and protected virtual machines.
- Acting as the vCenter Server management interface to the cluster and reporting the cluster health state.

The secondary hosts primarily contribute to the cluster by running virtual machines locally, monitoring their runtime states, and reporting state updates to the primary host. A primary host can also run and monitor virtual machines. Both secondary hosts and primary hosts implement the VM and Application Monitoring features.

One of the functions performed by the primary host is to orchestrate restarts of protected virtual machines. A virtual machine is protected by a primary host after vCenter Server observes that the virtual machine's power state has changed from powered off to powered on in response to a user action. The primary host persists the list of protected virtual machines in the cluster's datastores. A newly elected primary host uses this information to determine which virtual machines to protect.

Note: If you disconnect a host from a cluster, the virtual machines registered to that host are unprotected by vSphere HA.

Host Failure Types

The primary host of a VMware vSphere® High Availability cluster is responsible for detecting the failure of secondary hosts. Depending on the type of failure detected, the virtual machines running on the hosts might need to be failed over.

In a vSphere HA cluster, three types of host failure are detected:

- Failure. A host stops functioning.
- Isolation. A host becomes network isolated.
- Partition. A host loses network connectivity with the primary host.

The primary host monitors the liveness of the secondary hosts in the cluster. This communication happens through the exchange of network heartbeats every second. When the primary host stops receiving these heartbeats from a secondary host, it checks for host liveness before declaring the host failed. The liveness check that the primary host performs is to determine whether the secondary host is exchanging heartbeats with one of the datastores. See Datastore Heartbeating . Also, the primary host checks whether the host responds to ICMP pings sent to its management IP addresses.

If a primary host cannot communicate directly with the agent on a secondary host, the secondary host does not respond to ICMP pings. If the agent is not issuing heartbeats, it is viewed as failed. The host's virtual machines are restarted on alternate hosts. If such a secondary host is exchanging heartbeats with a datastore, the primary host assumes that the secondary host is in a network partition or is network isolated. So, the primary host continues to monitor the host and its virtual machines. See Network Partitions .

Host network isolation occurs when a host is still running, but it can no longer observe traffic from vSphere HA agents on the management network. If a host stops observing this traffic, it attempts to ping the cluster isolation addresses. If this pinging also fails, the host declares that it is isolated from the network.

The primary host monitors the virtual machines that are running on an isolated host. If the primary host observes that the VMs power off, and the primary host is responsible for the VMs, it restarts them.

Note: If you ensure that the network infrastructure is sufficiently redundant and that at least one network path is always available, host network isolation is less likely to occur.

Proactive HA Failures

A Proactive HA failure occurs when a host component fails, which results in a loss of redundancy or a noncatastrophic failure. However, the functional behavior of the VMs residing on the host is not yet affected. For example, if a power supply on the host fails, but other power supplies are available, that is a Proactive HA failure.

If a Proactive HA failure occurs, you can automate the remediation action taken in the vSphere Availability section of the vSphere Client. The VMs on the affected host can be evacuated to other hosts and the host is either placed in Quarantine mode or Maintenance mode.

Note: Your cluster must use vSphere DRS for the Proactive HA failure monitoring to work.

Determining Responses to Host Issues

If a host fails and its virtual machines must be restarted, you can control the order in which the virtual machines are restarted with the VM restart priority setting. You can also configure how vSphere HA responds if hosts lose management network connectivity with other hosts by using the host isolation response setting. Other factors are also considered when vSphere HA restarts a virtual machine after a failure.

The following settings apply to all virtual machines in the cluster in the case of a host failure or isolation. You can also configure exceptions for specific virtual machines. See Customize an Individual Virtual Machine .

Host Isolation Response

Host isolation response determines what happens when a host in a vSphere HA cluster loses its management network connections, but continues to run. You can use the isolation response to have vSphere HA power off virtual machines that are running on an isolated host and restart them on a non-isolated host. Host isolation responses require that Host Monitoring Status is activated. If Host Monitoring Status is deactivated, host isolation responses are also suspended. A host determines that it is isolated when it is unable to communicate with the agents running on the other hosts, and it is unable to ping its isolation addresses. The host then executes its isolation response. The responses are Power off and restart VMs or Shutdown and restart VMs. You can customize this property for individual virtual machines.

Note: If a virtual machine has a restart priority setting of Disabled, no host isolation response is made.

To use the Shutdown and restart VMs setting, you must install VMware Tools in the guest operating system of the virtual machine. Shutting down the virtual machine provides the advantage of preserving its state. Shutting down is better than powering off the virtual machine, which does not flush most recent changes to disk or commit transactions. Virtual machines that are in the process of shutting down take longer to fail over while the shutdown completes. Virtual Machines that have not shut down in 300 seconds, or the time specified in the advanced option das.isolationshutdowntimeout, are powered off.

After you create a vSphere HA cluster, you can override the default cluster settings for Restart Priority and Isolation Response for specific virtual machines. Such overrides are useful for virtual machines that are used for special tasks. For example, virtual machines that provide infrastructure services like DNS or DHCP might need to be powered on before other virtual machines in the cluster.

A virtual machine "split-brain" condition can occur when a host becomes isolated or partitioned from a primary host and the primary host cannot communicate with it using heartbeat datastores. In this situation, the primary host cannot determine that the host is alive and so declares it dead. The primary host then attempts to restart the virtual machines that are running on the isolated or partitioned host. This attempt succeeds if the virtual machines remain running on the isolated/partitioned host and that host lost access to the virtual machines' datastores when it became isolated or partitioned. A split-brain condition then exists because there are two instances of the virtual machine. However, only one instance is able to read or write the virtual machine's virtual disks. VM Component Protection can be used to prevent this split-brain condition. When you activate VMCP with the aggressive setting, it monitors the datastore accessibility of powered-on virtual machines, and shuts down those that lose access to their datastores.

To recover from this situation, ESXi generates a question on the virtual machine that has lost the disk locks for when the host comes out of isolation and cannot reacquire the disk locks. vSphere HA automatically answers this question, allowing the virtual machine instance that has lost the disk locks to power off, leaving just the instance that has the disk locks.

Virtual Machine Dependencies

You can create dependencies between groups of virtual machines. To do so, you must first create the VM groups in the vSphere Client by going to the **Configure** tab for the cluster and selecting **VM/Host Groups**. Once the groups have been created, you can create restart dependency rules between the groups by browsing to**VM/Host Rules** and in the Type drop-down menu, select **Virtual Machines to Virtual Machines**. These rules can specify that certain VM groups cannot be restarted until other, specified VM groups have been Ready first.

Factors Considered for Virtual Machine Restarts

After a failure, the cluster's primary host attempts to restart affected virtual machines by identifying a host that can power them on. When choosing such a host, the primary host considers a number of factors.

File accessibility	Before a virtual machine can be started, its files must be accessible from one of the active cluster hosts that the primary can communicate with over the network
Virtual machine and host compatibility	If there are accessible hosts, the virtual machine must be compatible with at least one of them. The compatibility set for a virtual machine includes the effect of any required VM-Host affinity

	rules. For example, if a rule only permits a virtual machine to run on two hosts, it is considered for placement on those two hosts.
Resource reservations	Of the hosts that the virtual machine can run on, at least one must have sufficient unreserved capacity to meet the memory overhead of the virtual machine and any resource reservations. Four types of reservations are considered: CPU, Memory, vNIC, and Virtual flash. Also, sufficient network ports must be available to power on the virtual machine.
Host limits	In addition to resource reservations, a virtual machine can only be placed on a host if doing so does not violate the maximum number of allowed virtual machines or the number of in-use vCPUs.
Feature constraints	If the advanced option has been set that requires vSphere HA to enforce VM to VM anti-affinity rules, vSphere HA does not violate this rule. Also, vSphere HA does not violate any configured per host limits for fault tolerant virtual machines.

If no hosts satisfy the preceding considerations, the primary host issues an event stating that there are not enough resources for vSphere HA to start the VM and tries again when the cluster conditions have changed. For example, if the virtual machine is not accessible, the primary host tries again after a change in file accessibility.

VM and Application Monitoring

VM Monitoring restarts individual virtual machines if their VMware Tools heartbeats are not received within a set time. Similarly, Application Monitoring can restart a virtual machine if the heartbeats for an application it is running are not received. You can enable these features and configure the sensitivity with which vSphere HA monitors non-responsiveness.

When you enable VM Monitoring, the VM Monitoring service (using VMware Tools) evaluates whether each virtual machine in the cluster is running by checking for regular heartbeats and I/O activity from the VMware Tools process running inside the guest. If no heartbeats or I/O activity are received, this is most likely because the guest operating system has failed or VMware Tools is not being allocated any time to complete tasks. In such a case, the VM Monitoring service determines that the virtual machine has failed and the virtual machine is rebooted to restore service. For information on how to enable VM monitoring, see Activate VM Monitoring.

Occasionally, virtual machines or applications that are still functioning properly stop sending heartbeats. To avoid unnecessary resets, the VM Monitoring service also monitors a virtual machine's I/O activity. If no heartbeats are received within the failure interval, the I/O stats interval (a cluster-level attribute) is checked. The I/O stats interval determines if any disk or network activity has occurred for the virtual machine during the previous two minutes (120 seconds). If not, the virtual machine is reset. This default value (120 seconds) can be changed using the advanced option das.iostatsinterval.

To enable Application Monitoring, you must first obtain the appropriate SDK (or be using an application that supports VMware Application Monitoring) and use it to set up customized heartbeats for the applications you want to monitor. After you have done this, Application Monitoring works much the same way that VM Monitoring does. If the heartbeats for an application are not received for a specified time, its virtual machine is restarted.

You can configure the level of monitoring sensitivity. Highly sensitive monitoring results in a more rapid conclusion that a failure has occurred. While unlikely, highly sensitive monitoring might lead to falsely identifying failures when the virtual machine or application in question is actually still working, but heartbeats have not been received due to factors such as resource constraints. Low sensitivity monitoring results in longer interruptions in service between actual failures and virtual machines being reset. Select an option that is an effective compromise for your needs.

You can also specify custom values for the monitoring sensitivity interval by selecting the **Custom** check box.

Table 344: VM Monitoring Settings

Preset Setting	Failure interval (seconds)	Minimum uptime (seconds)	Maximum per-VM resets	Maximum resets time window (hours)
High	30	120	3	1
Medium	60	240	3	24
Low	120	480	3	168

- **Failure interval**: If no VM heartbeat is received in the specified interval, vSphere HA restarts the VM.
- **Minimum uptime**: After a VM starts, vSphere HA waits until the specified interval is reached, before monitoring for VM heartbeats, storage and network traffic.
- **Maximum per-VM resets**: The maximum number of resets, that vSphere HA can restart a VM a within the specified interval for **Maximum resets time window**.
- **Maximum reset time window**: The maximum interval for the number of specified **Maximum per-VM resets**.

Note: To set a custom value for the I/O stats interval, you can use the `das.iostatsInterval` advanced configuration option. For more information, see kB 2033250.

After failures are detected, vSphere HA resets virtual machines. The reset ensures that services remain available. To avoid resetting virtual machines repeatedly for nontransient errors, by default, virtual machines will be reset only three times during a certain configurable time interval. After virtual machines have been reset three times, vSphere HA makes no further attempts to reset the virtual machines after subsequent failures until after the specified time has elapsed. You can configure the number of resets using the **Maximum per-VM resets** custom setting.

Note: The reset statistics are cleared when a virtual machine is powered off then back on, or when it is migrated using vMotion to another host. This causes the guest operating system to reboot, but is not the same as a 'restart' in which the power state of the virtual machine is changed.

VM Component Protection

If VM Component Protection (VMCP) is activated, vSphere HA can detect datastore accessibility failures and provide automated recovery for affected virtual machines.

VMCP provides protection against datastore accessibility failures that can affect a virtual machine running on a host in a vSphere HA cluster. When a datastore accessibility failure occurs, the affected host can no longer access the storage path for a specific datastore. You can determine the response that vSphere HA will make to such a failure, ranging from the creation of event alarms to virtual machine restarts on other hosts.

Note: When you use the VM Component Protection feature, your ESXi hosts must be version 6.0 or higher.

Types of Failure

There are two types of datastore accessibility failure:

PDL	PDL (Permanent Device Loss) is an unrecoverable loss of accessibility that occurs when a storage device reports the datastore is no longer accessible by the host. This condition cannot be reverted without powering off virtual machines.
APD	APD (All Paths Down) represents a transient or unknown accessibility loss or any other unidentified delay in I/O processing. This type of accessibility issue is recoverable.

Configuring VMCP

VM Component Protection is configured in the vSphere Client. Go to the **Configure** tab and click **vSphere Availability** and **Edit**. Under **Failures and Responses** you can select **Datastore with PDL** or **Datastore with APD**. The storage protection levels you can choose and the virtual machine remediation actions available differ depending on the type of database accessibility failure.

PDL Failures	Under **Datastore with PDL**, you can select **Issue events** or **Power off and restart VMs**.
APD Failures	The response to APD events is more complex and accordingly the configuration is more fine-grained. You can select **Issue events**, **Power off and restart VMs--conservative restart policy**, or **Power off and restart VMs--aggressive restart policy**

Note: If either the Host Monitoring or VM Restart Priority settings are deactivated, VMCP cannot perform virtual machine restarts. Storage health can still be monitored and events can be issued, however.

Network Partitions

When a management network failure occurs for a vSphere HA cluster, a subset of the cluster's hosts might be unable to communicate over the management network with the other hosts. Multiple partitions can occur in a cluster.

A partitioned cluster leads to degraded virtual machine protection and cluster management functionality. Correct the partitioned cluster as soon as possible.

- Virtual machine protection. vCenter Server allows a virtual machine to be powered on, but it can be protected only if it is running in the same partition as the primary host that is responsible for it. The primary host must be communicating with vCenter Server. A primary host is responsible for a virtual machine if it has exclusively locked a system-defined file on the datastore that contains the virtual machine's configuration file.
- Cluster management. vCenter Server can communicate with the primary host, but only a subset of the secondary hosts. As a result, changes in configuration that affect vSphere HA might not take effect until after the partition is resolved. This failure could result in one of the partitions operating under the old configuration, while another uses the new settings.

Datastore Heartbeating

When the primary host in a VMware vSphere® High Availability cluster cannot communicate with a secondary host over the management network, the primary host uses datastore heartbeating to determine whether the secondary host has failed, is in a network partition, or is network isolated. If the secondary host has stopped datastore heartbeating, it is considered to have failed and its virtual machines are restarted elsewhere.

VMware vCenter Server® selects a preferred set of datastores for heartbeating. This selection is made to maximize the number of hosts that have access to a heartbeating datastore and minimize the likelihood that the datastores are backed by the same LUN or NFS server.

You can use the advanced option das.heartbeatdsperhost to change the number of heartbeat datastores selected by vCenter Server for each host. The default is two and the maximum valid value is five.

vSphere HA creates a directory at the root of each datastore that is used for both datastore heartbeating and for persisting the set of protected virtual machines. The name of the directory is `.vSphere-HA`. Do not delete or modify the files stored in this directory, because this can have an impact on operations. Because more than one cluster might use a datastore, subdirectories for this directory are created for each cluster. Root owns these directories and files and only root can read and write to them. The disk space used by vSphere HA depends on several factors including which VMFS version is in use and the number of hosts that use the datastore for heartbeating. With vmfs3, the maximum usage is 2GB and the typical usage is 3MB. With vmfs5 and vmfs6, the maximum and typical usage is 3MB. vSphere HA use of the datastores adds negligible overhead and has no performance impact on other datastore operations.

vSphere HA limits the number of virtual machines that can have configuration files on a single datastore. See *Configuration Maximums* for updated limits. If you place more than this number of virtual machines on a datastore and power them on, vSphere HA protects virtual machines only up to the limit.

Note: A vSAN datastore cannot be used for datastore heartbeating. Therefore, if no other shared storage is accessible to all hosts in the cluster, there can be no heartbeat datastores in use. However, if you have storage that is accessible by an alternate network path independent of the vSAN network, you can use it to set up a heartbeat datastore.

vSphere HA Security

vSphere HA is enhanced by several security features.

Select firewall ports opened	vSphere HA uses TCP and UDP port 8182 for agent-to-agent communication. The firewall ports open and close automatically to ensure they are open only when needed.
Configuration files protected using file system permissions	vSphere HA stores configuration information on the local storage or on ramdisk if there is no local datastore. These files are protected using file system permissions and they are accessible only to the root user. Hosts without local storage are only supported if they are managed by Auto Deploy.
Detailed logging	The location where vSphere HA places log files depends on the version of host. • For ESXi hosts, vSphere HA writes to syslog only by default, so logs are placed where syslog is configured to put them. The log file names for vSphere HA are prepended with `fdm`, fault domain manager, which is a service of vSphere HA. • For legacy ESXi hosts, vSphere HA writes to `/var/log/vmware/fdm` on local disk, as well as syslog if it is configured.
Secure vSphere HA logins	vSphere HA logs onto the vSphere HA agents using a user account, **vpxuser**, created by vCenter Server. This account is the same account used by vCenter Server to manage the host. vCenter Server creates a random password for this account and changes the password periodically. The time period is set by the vCenter Server VirtualCenter.VimPasswordExpirationInDays setting. Users with administrative privileges on the root folder of the host can log in to the agent.
Secure communication	All communication between vCenter Server and the vSphere HA agent is done over SSL. Agent-to-agent communication also uses SSL except for election messages, which occur over UDP. Election messages are verified over SSL so that a rogue agent can prevent only the host on which the agent is running from being elected as a primary host. In this case, a configuration issue for the cluster is issued so the user is aware of the problem.
Host SSL certificate verification required	vSphere HA requires that each host have a verified SSL certificate. Each host generates a self-signed certificate when it is booted for the first time. This certificate can then be regenerated or replaced with one issued by an authority. If the certificate is replaced, vSphere HA needs to be reconfigured on the host. If a host becomes disconnected from vCenter Server after its certificate is updated and the ESXi or ESX Host agent is restarted, then vSphere HA is automatically reconfigured when the host is reconnected to vCenter Server. If the disconnection does not occur because vCenter Server host SSL certificate verification is deactivated at the time, verify the new certificate and reconfigure vSphere HA on the host.

vSphere HA Admission Control

vSphere HA uses admission control to ensure that sufficient resources are reserved for virtual machine recovery when a host fails.

Admission control imposes constraints on resource usage. Any action that might violate these constraints is not permitted. Actions that might be disallowed include the following examples:

- Powering on a virtual machine
- Migrating a virtual machine
- Increasing the CPU or memory reservation of a virtual machine

The basis for vSphere HA admission control is how many host failures your cluster is allowed to tolerate and still guarantee failover. The host failover capacity can be set in three ways:

- Cluster resource percentage
- Slot policy
- Dedicated failover hosts

Note: vSphere HA admission control can be deactivated. However, without it you have no assurance that the expected number of virtual machines can be restarted after a failure. Do not permanently deactivate admission control.

Note: To use vSphere HA admission control you must have at least 3 hosts in the cluster.

Regardless of the admission control option chosen, a VM resource reduction threshold also exists. You use this setting to specify the percentage of resource degradation to tolerate, but it is not available unless vSphere DRS is activated.

The resource reduction calculation is checked for both CPU and memory. It considers a virtual machine's reserved memory and memory overload to decide whether to permit it to power on, migrate, or have reservation changes. The actual memory consumed by the virtual machine is not considered in the calculation because the memory reservation does not always correlate with the actual memory usage of the virtual machine. If the actual usage is more than reserved memory, insufficient failover capacity is available, resulting in performance degradation on failover.

Setting a performance reduction threshold allows you to specify the occurrence of a configuration issue. For example:

- The default value is 100%, which produces no warnings.
- If you reduce the threshold to 0%, a warning is generated when cluster usage exceeds the available capacity.
- If you reduce the threshold to 20%, the performance reduction that can be tolerated is calculated as `performance reduction = current utilization * 20%`. When the current usage minus the performance reduction exceeds the available capacity, a configuration notice is issued.

Cluster Resources Percentage Admission Control

You can configure vSphere HA to perform admission control by reserving a specific percentage of cluster CPU and memory resources for recovery from host failures.

With this type of admission control, vSphere HA ensures that a specified percentage of aggregate CPU and memory resources are reserved for failover.

With the cluster resources percentage option, vSphere HA enforces admission control as follows:

1. Calculates the total resource requirements for all powered-on virtual machines in the cluster.
2. Calculates the total host resources available for virtual machines.
3. Calculates the Current CPU Failover Capacity and Current Memory Failover Capacity for the cluster.
4. Determines if either the Current CPU Failover Capacity or Current Memory Failover Capacity is less than the corresponding Configured Failover Capacity (provided by the user).
   If so, admission control disallows the operation.

vSphere HA uses the actual reservations of the virtual machines. If a virtual machine does not have reservations, meaning that the reservation is 0, a default of 0MB memory and 32MHz CPU is applied.

Note: The cluster resources percentage option for admission control also checks that there are at least two vSphere HA-enabled hosts in the cluster (excluding hosts that are entering maintenance mode). If there is only one vSphere HA-enabled host, an operation is not allowed, even if there is a sufficient percentage of resources available. The reason for this extra check is that vSphere HA cannot perform failover if there is only a single host in the cluster.

Computing the Current Failover Capacity

The total resource requirements for the powered-on virtual machines is comprised of two components, CPU and memory. vSphere HA calculates these values.

- The CPU component by summing the CPU reservations of the powered-on virtual machines. If you have not specified a CPU reservation for a virtual machine, it is assigned a default value of 32MHz (this value can be changed using the das.vmcpuminmhz advanced option.)
- The memory component by summing the memory reservation (plus memory overhead) of each powered-on virtual machine.

The total host resources available for virtual machines is calculated by adding the hosts' CPU and memory resources. These amounts are those contained in the host's root resource pool, not the total physical resources of the host. Resources being used for virtualization purposes are not included. Only hosts that are connected, not in maintenance mode, and have no vSphere HA errors are considered.

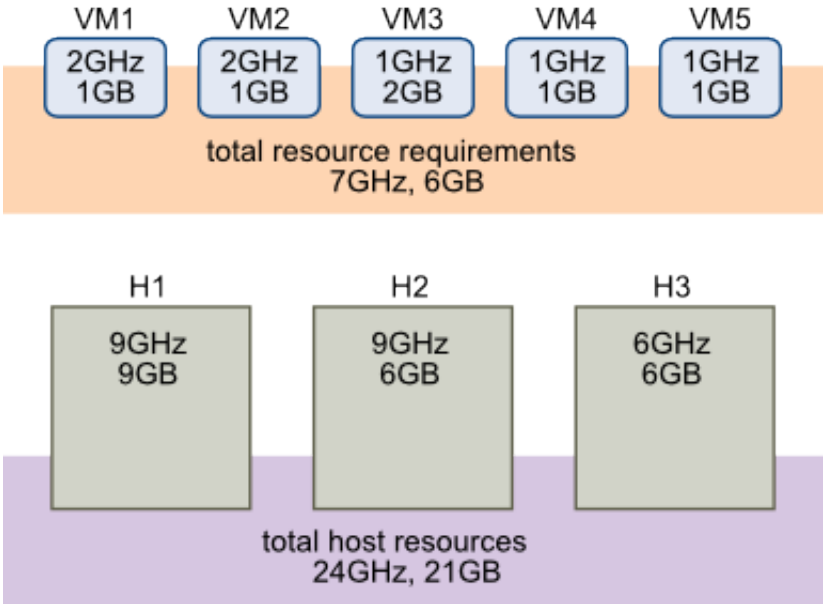
The Current CPU Failover Capacity is computed by subtracting the total CPU resource requirements from the total host CPU resources and dividing the result by the total host CPU resources. The Current Memory Failover Capacity is calculated similarly.

Admission Control Using Cluster Resources Percentage

The way that Current Failover Capacity is calculated and used with this admission control policy is shown with an example. Make the following assumptions about a cluster:

- The cluster is comprised of three hosts, each with a different amount of available CPU and memory resources. The first host (H1) has 9GHz of available CPU resources and 9GB of available memory, while Host 2 (H2) has 9GHz and 6GB and Host 3 (H3) has 6GHz and 6GB.
- There are five powered-on virtual machines in the cluster with differing CPU and memory requirements. VM1 needs 2GHz of CPU resources and 1GB of memory, while VM2 needs 2GHz and 1GB, VM3 needs 1GHz and 2GB, VM4 needs 1GHz and 1GB, and VM5 needs 1GHz and 1GB.
- The Configured Failover Capacity for CPU and Memory are both set to 25%.

Figure 109: Admission Control Example with Percentage of Cluster Resources Reserved Policy



The total resource requirements for the powered-on virtual machines is 7GHz and 6GB. The total host resources available for virtual machines is 24GHz and 21GB. Based on this, the Current CPU Failover Capacity is 70% ((24GHz - 7GHz)/24GHz). Similarly, the Current Memory Failover Capacity is 71% ((21GB-6GB)/21GB).

Because the cluster's Configured Failover Capacity is set to 25%, 45% of the cluster's total CPU resources and 46% of the cluster's memory resources are still available to power on additional virtual machines.

Slot Policy Admission Control

With the slot policy option, vSphere HA admission control ensures that a specified number of hosts can fail and sufficient resources remain in the cluster to fail over all the virtual machines from those hosts.

Using the slot policy, vSphere HA performs admission control in the following way:

1. Calculates the slot size.
   A slot is a logical representation of memory and CPU resources. By default, it is sized to satisfy the requirements for any powered-on virtual machine in the cluster.
2. Determines how many slots each host in the cluster can hold.
3. Determines the Current Failover Capacity of the cluster.
   This is the number of hosts that can fail and still leave enough slots to satisfy all of the powered-on virtual machines.
4. Determines whether the Current Failover Capacity is less than the Configured Failover Capacity (provided by the user).
   If it is, admission control disallows the operation.

Note: You can set a specific slot size for both CPU and memory in the admission control section of the vSphere HA settings in the vSphere Client.

Slot Size Calculation

Slot size is comprised of two components, CPU and memory.

- vSphere HA calculates the CPU component by obtaining the CPU reservation of each powered-on virtual machine and selecting the largest value. If you have not specified a CPU reservation for a virtual machine, it is assigned a default value of 32MHz. You can change this value by using the das.vmcpuminmhz advanced option.)
- vSphere HA calculates the memory component by obtaining the memory reservation, plus memory overhead, of each powered-on virtual machine and selecting the largest value. There is no default value for the memory reservation.

If your cluster contains any virtual machines that have much larger reservations than the others, they will distort slot size calculation. To avoid this, you can specify an upper bound for the CPU or memory component of the slot size by using the das.slotcpuinmhz or das.slotmeminmb advanced options, respectively. See vSphere HA Advanced Options.

You can also determine the risk of resource fragmentation in your cluster by viewing the number of virtual machines that require multiple slots. This can be calculated in the admission control section of the vSphere HA settings in the vSphere Client. Virtual machines might require multiple slots if you have specified a fixed slot size or a maximum slot size using advanced options.

Using Slots to Compute the Current Failover Capacity

After the slot size is calculated, vSphere HA determines each host's CPU and memory resources that are available for virtual machines. These amounts are those contained in the host's root resource pool, not the total physical resources of the host. The resource data for a host that is used by vSphere HA can be found on the host's **Summary** tab on the vSphere Client. If all hosts in your cluster are the same, this data can be obtained by dividing the cluster-level figures by the number of hosts. Resources being used for virtualization purposes are not included. Only hosts that are connected, not in maintenance mode, and that have no vSphere HA errors are considered.

The maximum number of slots that each host can support is then determined. To do this, the host’s CPU resource amount is divided by the CPU component of the slot size and the result is rounded down. The same calculation is made for the host's memory resource amount. These two numbers are compared and the smaller number is the number of slots that the host can support.

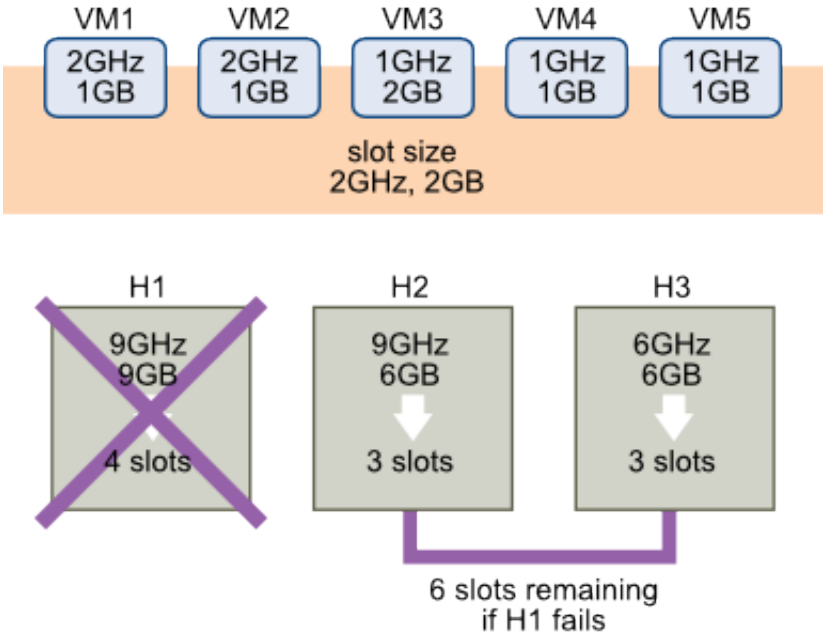
The Current Failover Capacity is computed by determining how many hosts (starting from the largest) can fail and still leave enough slots to satisfy the requirements of all powered-on virtual machines.

Admission Control Using Slot Policy

The way that slot size is calculated and used with this admission control policy is shown in an example. Make the following assumptions about a cluster:

- The cluster is comprised of three hosts, each with a different amount of available CPU and memory resources. The first host (H1) has 9GHz of available CPU resources and 9GB of available memory, while Host 2 (H2) has 9GHz and 6GB and Host 3 (H3) has 6GHz and 6GB.
- There are five powered-on virtual machines in the cluster with differing CPU and memory requirements. VM1 needs 2GHz of CPU resources and 1GB of memory, while VM2 needs 2GHz and 1GB, VM3 needs 1GHz and 2GB, VM4 needs 1GHz and 1GB, and VM5 needs 1GHz and 1GB.
- The Host Failures Cluster Tolerates is set to one.

Figure 110: Admission Control Example with Host Failures Cluster Tolerates Policy



1. Slot size is calculated by comparing both the CPU and memory requirements of the virtual machines and selecting the largest.
   The largest CPU requirement (shared by VM1 and VM2) is 2GHz, while the largest memory requirement (for VM3) is 2GB. Based on this, the slot size is 2GHz CPU and 2GB memory.
2. Maximum number of slots that each host can support is determined.
   H1 can support four slots. H2 can support three slots (which is the smaller of 9GHz/2GHz and 6GB/2GB) and H3 can also support three slots.
3. Current Failover Capacity is computed.
   The largest host is H1 and if it fails, six slots remain in the cluster, which is sufficient for all five of the powered-on virtual machines. If both H1 and H2 fail, only three slots remain, which is insufficient. Therefore, the Current Failover Capacity is one.

The cluster has one available slot (the six slots on H2 and H3 minus the five used slots).

Dedicated Failover Hosts Admission Control

You can configure vSphere HA to designate specific hosts as the failover hosts.

With dedicated failover hosts admission control, when a host fails, vSphere HA attempts to restart its virtual machines on any of the specified failover hosts. If restarting the virtual machines is not possible, for example the failover hosts have failed or have insufficient resources, then vSphere HA attempts to restart those virtual machines on other hosts in the cluster.

To ensure that spare capacity is available on a failover host, you are prevented from powering on virtual machines or using vMotion to migrate virtual machines to a failover host. Also, DRS does not use a failover host for load balancing.

Note: If you use dedicated failover hosts admission control and designate multiple failover hosts, DRS does not attempt to enforce VM-VM affinity rules for virtual machines that are running on failover hosts.

vSphere HA Interoperability

vSphere HA can interoperate with many other features, such as DRS and vSAN.

Before configuring vSphere HA, you should be aware of the limitations of its interoperability with these other features or products.

Using vSphere HA with vSAN

You can use vSAN as the shared storage for a vSphere HA cluster. If activated, vSAN aggregates the specified local storage disks available on the hosts into a single datastore shared by all hosts.

To use vSphere HA with vSAN, you must be aware of certain considerations and limitations for the interoperability of these two features.

For information about vSAN, see *Administering VMware vSAN*.

Note: You can use vSphere HA with vSAN stretched clusters.

ESXi Host Requirements

You can use vSAN with a vSphere HA cluster only if the following conditions are met:

- All the cluster's ESXi hosts must be version 5.5 or later.
- The cluster must have a minimum of three ESXi hosts.

Networking Differences

vSAN has its own network. If vSAN and vSphere HA are activated for the same cluster, the HA interagent traffic flows over this storage network rather than the management network. vSphere HA uses the management network only if vSAN is deactivated. vCenter Server chooses the appropriate network if vSphere HA is configured on a host.

Note: You can activate vSAN only if vSphere HA is deactivated.

If you change the vSAN network configuration, the vSphere HA agents do not automatically pick up the new network settings. To make changes to the vSAN network, you must take the following steps in the vSphere Client:

1. Deactivate Host Monitoring for the vSphere HA cluster.
2. Make the vSAN network changes.
3. Right-click all hosts in the cluster and select **Reconfigure for vSphere HA**.
4. Re-activate Host Monitoring for the vSphere HA cluster.

The following table shows the differences in vSphere HA networking whether or not vSAN is used.

Table 345: vSphere HA Networking Differences

	vSAN Activated	vSAN Deactivated
Network used by vSphere HA	vSAN storage network	Management network
Heartbeat datastores	Any datastore mounted to > 1 host, but not vSAN datastores	Any datastore mounted to > 1 host
Host declared isolated	Isolation addresses not pingable and vSAN storage network inaccessible	Isolation addresses not pingable and management network inaccessible

Capacity Reservation Settings

When you reserve capacity for your vSphere HA cluster with an admission control policy, you must coordinate this setting with the corresponding vSAN setting that ensures data accessibility on failures. Specifically, the Number of Failures Tolerated setting in the vSAN rule set must not be lower than the capacity that the vSphere HA admission control setting reserved.

For example, if the vSAN rule set allows for only two failures, the vSphere HA admission control policy must reserve capacity that is equivalent to only one or two host failures. If you are using the Percentage of Cluster Resources Reserved policy for a cluster that has eight hosts, you must not reserve more than 25% of the cluster resources. In the same cluster, with the Host Failures Cluster Tolerates policy, the setting must not be higher than two hosts. If vSphere HA reserves less capacity, failover activity might be unpredictable. Reserving too much capacity overly constrains the powering on of virtual machines and intercluster vSphere vMotion migrations.

Using vSphere HA and DRS Together

Using vSphere HA with Distributed Resource Scheduler (DRS) combines automatic failover with load balancing. This combination can result in a more balanced cluster after vSphere HA has moved virtual machines to different hosts.

When vSphere HA performs failover and restarts virtual machines on different hosts, its first priority is the immediate availability of all virtual machines. After the virtual machines have been restarted, those hosts on which they were powered on might be heavily loaded, while other hosts are comparatively lightly loaded. vSphere HA uses the virtual machine's CPU and memory reservation and overhead memory to determine if a host has enough spare capacity to accommodate the virtual machine.

In a cluster using DRS and vSphere HA with admission control turned on, virtual machines might not be evacuated from hosts entering maintenance mode. This behavior occurs because of the resources reserved for restarting virtual machines in the event of a failure. You must manually migrate the virtual machines off of the hosts using vMotion.

In some scenarios, vSphere HA might not be able to fail over virtual machines because of resource constraints. This can occur for several reasons.

- HA admission control is deactivated and Distributed Power Management (DPM) is activated. This can result in DPM consolidating virtual machines onto fewer hosts and placing the empty hosts in standby mode leaving insufficient powered-on capacity to perform a failover.
- VM-Host affinity (required) rules might limit the hosts on which certain virtual machines can be placed.
- There might be sufficient aggregate resources but these can be fragmented across multiple hosts so that they can not be used by virtual machines for failover.

In such cases, vSphere HA can use DRS to try to adjust the cluster (for example, by bringing hosts out of standby mode or migrating virtual machines to defragment the cluster resources) so that HA can perform the failovers.

If DPM is in manual mode, you might need to confirm host power-on recommendations. Similarly, if DRS is in manual mode, you might need to confirm migration recommendations.

If you are using VM-Host affinity rules that are required, be aware that these rules cannot be violated. vSphere HA does not perform a failover if doing so would violate such a rule.

For more information about DRS, see the *vSphere Resource Management* documentation.

Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See *vSphere Cluster Services (vCLS)* in *vSphere Resource Management* for more information.

vSphere HA and DRS Affinity Rules

If you create a DRS affinity rule for your cluster, you can specify how vSphere HA applies that rule during a virtual machine failover.

The two types of rules for which you can specify vSphere HA failover behavior are the following:

- VM anti-affinity rules force specified virtual machines to remain apart during failover actions.
- VM-Host affinity rules place specified virtual machines on a particular host or a member of a defined group of hosts during failover actions.

When you edit a DRS affinity rule, you must use vSphere HA advanced options to enforce the desired failover behavior for vSphere HA.

- **HA must respect VM anti-affinity rules during failover** -- When the advanced option for VM anti-affinity rules is set, vSphere HA does not fail over a virtual machine if doing so violates a rule. Instead, vSphere HA issues an event reporting there are insufficient resources to perform the failover.
- **HA should respect VM to Host affinity rules during failover** --vSphere HA attempts to place VMs with this rule on the specified hosts if at all possible.

For more information, see vSphere HA Advanced Options.

Note: vSphere HA can restart a VM in a DRS-deactivated cluster, overriding a VM-Host affinity rules mapping if the host failure happens soon (by default, within 5 minutes) after setting the rule.

Other vSphere HA Interoperability Issues

To use vSphere HA, you must be aware of the following additional interoperability issues.

VM Component Protection

VM Component Protection (VMCP) has the following interoperability issues and limitations:

- VMCP does not support vSphere Fault Tolerance. If VMCP is activated for a cluster using Fault Tolerance, the affected FT virtual machines will automatically receive overrides that deactivate VMCP.
- VMCP does not detect or respond to accessibility issues for files located on vSAN datastores. If a virtual machine's configuration and VMDK files are located only on vSAN datastores, they are not protected by VMCP.
- VMCP does not detect or respond to accessibility issues for files located on Virtual Volume datastores. If a virtual machine's configuration and VMDK files are located only on Virtual Volume datastores, they are not protected by VMCP.
- VMCP does not protect against inaccessible Raw Device Mapping (RDM)s.

IPv6

vSphere HA can be used with IPv6 network configurations, which are fully supported if the following considerations are observed:

- The cluster contains only ESXi 6.0 or later hosts.
- The management network for all hosts in the cluster must be configured with the same IP version, either IPv6 or IPv4. vSphere HA clusters cannot contain both types of networking configuration.
- The network isolation addresses used by vSphere HA must match the IP version used by the cluster for its management network.
- IPv6 cannot be used in vSphere HA clusters that also utilize vSAN.

In addition to the previous restrictions, the following types of IPv6 address types are not supported for use with the vSphere HA isolation address or management network: link-local, ORCHID, and link-local with zone indices. Also, the loopback address type cannot be used for the management network.

Note: To upgrade an existing IPv4 deployment to IPv6, you must first deactivate vSphere HA.

Creating a vSphere HA Cluster

vSphere HA operates in the context of a cluster of ESXi (or legacy ESX) hosts. You must create a cluster, populate it with hosts, and configure vSphere HA settings before failover protection can be established.

When you create a vSphere HA cluster, you must configure a number of settings that determine how the feature works. Before you do this, identify your cluster's nodes. These nodes are the ESXi hosts that will provide the resources to support virtual machines and that vSphere HA will use for failover protection. You should then determine how those nodes are to be connected to one another and to the shared storage where your virtual machine data resides. After that networking architecture is in place, you can add the hosts to the cluster and finish configuring vSphere HA.

You can activate and configure vSphere HA before you add host nodes to the cluster. However, until the hosts are added, your cluster is not fully operational and some of the cluster settings are unavailable. For example, the Specify a Failover Host admission control policy is unavailable until there is a host that can be designated as the failover host.

Note: The Virtual Machine Startup and Shutdown (automatic startup) feature is deactivated for all virtual machines residing on hosts that are in (or moved into) a vSphere HA cluster. Automatic startup is not supported when used with vSphere HA.

vSphere HA Checklist

The vSphere HA checklist contains requirements that you must be aware of before creating and using a vSphere HA cluster.

Review this list before you set up a vSphere HA cluster. For more information, follow the appropriate cross reference.

- All hosts must be licensed for vSphere HA.
- A cluster must contain at least two hosts.
- All hosts must be configured with static IP addresses. If you are using DHCP, you must ensure that the address for each host persists across reboots.
- All hosts must have at least one management network in common. The best practice is to have at least two management networks in common. You should use the VMkernel network with the **Management traffic** checkbox enabled. The networks must be accessible to each other and vCenter Server and the hosts must be accessible to each other on the management networks. SeeBest Practices for Networking.
- To ensure that any virtual machine can run on any host in the cluster, all hosts must have access to the same virtual machine networks and datastores. Similarly, virtual machines must be located on shared, not local, storage otherwise they cannot be failed over in the case of a host failure.

  Note: vSphere HA uses datastore heartbeating to distinguish between partitioned, isolated, and failed hosts. So if some datastores are more reliable in your environment, configure vSphere HA to give preference to them.
- For VM Monitoring to work, VMware tools must be installed. See VM and Application Monitoring.
- vSphere HA supports both IPv4 and IPv6. See Other vSphere HA Interoperability Issues for considerations when using IPv6.
- For VM Component Protection to work, hosts must have the All Paths Down (APD) Timeout feature enabled.
- To use VM Component Protection, clusters must contain ESXi 6.0 hosts or later.
- Only vSphere HA clusters that contain ESXi 6.0 or later hosts can be used to enable VMCP. Clusters that contain hosts from an earlier release cannot enable VMCP, and such hosts cannot be added to a VMCP-enabled cluster.
- If your cluster uses Virtual Volume datastores, when vSphere HA is enabled a configuration Virtual Volume is created on each datastore by vCenter Server. In these containers, vSphere HA stores the files it uses to protect virtual machines. vSphere HA does not function correctly if you delete these containers. Only one container is created per Virtual Volume datastore.

Create a vSphere HA Cluster in the vSphere Client

To enable your cluster for vSphere HA, you must first create an empty cluster. After you plan the resources and networking architecture of your cluster, use the vSphere Client to add hosts to the cluster and specify the cluster's vSphere HA settings.

- Verify that all virtual machines and their configuration files reside on shared storage.
- Verify that the hosts are configured to access the shared storage so that you can power on the virtual machines by using different hosts in the cluster.
- Verify that hosts are configured to have access to the virtual machine network.
- Verify that you are using redundant management network connections for vSphere HA. For information about setting up network redundancy, see Best Practices for Networking.
- Verify that you have configured hosts with at least two datastores to provide redundancy for vSphere HA datastore heartbeating.
- Connect vSphere Client to vCenter Server by using an account with cluster administrator permissions.

A vSphere HA-enabled cluster is a prerequisite for vSphere Fault Tolerance.

1. In the vSphere Client, browse to the data center where you want the cluster to reside and click **New Cluster**.
2. Complete the **New Cluster** wizard.

   Do not turn on vSphere HA (or DRS).
3. Click **OK** to close the wizard and create an empty cluster.
4. Based on your plan for the resources and networking architecture of the cluster, use the vSphere Client to add hosts to the cluster.
5. Browse to the cluster and enable vSphere HA.
   a) Click the **Configure** tab.
   b) Select **vSphere Availability** and click **Edit**.
   c) Select **vSphere HA**.
6. Under **Failures and Responses** select **Enable Host Monitoring**.

   With Host Monitoring enabled, hosts in the cluster can exchange network heartbeats and vSphere HA can take action when it detects failures. Host Monitoring is required for the vSphere Fault Tolerance recovery process to work properly.
7. Select a setting for **VM Monitoring**.

   Select **VM Monitoring Only** to restart individual virtual machines if their heartbeats are not received within a set time. You can also select **VM and Application Monitoring** to enable application monitoring.
8. Click **OK**.

You have a vSphere HA cluster, populated with hosts.

Configure the appropriate vSphere HA settings for your cluster.

- Failures and responses
- Admission Control
- Heartbeat Datastores
- Advanced Options

See Configuring vSphere Availability Settings.

Configuring vSphere Availability Settings

When you create a vSphere HA cluster or configure an existing cluster, you must configure settings that determine how the feature works.

In the vSphere Client, you can configure following the vSphere HA settings:

Failures and responses	Provide settings here for host failure responses, host isolation, VM monitoring, and VM Component Protection.
Admission Control	Activate or deactivate admission control for the vSphere HA cluster and choose a policy for how it is enforced.
Heartbeat Datastores	Specify preferences for the datastores that vSphere HA uses for datastore heartbeating.
Advanced Options	Customize vSphere HA behavior by setting advanced options.

Configuring Responses to Failures

The **Failure and Responses** pane of the vSphere HA settings allows you to configure how your cluster should function when problems are encountered.

In this part of the vSphere Client, you can determine the specific responses the vSphere HA cluster has for host failures and isolation. You can also configure VM Component Protection (VMCP) actions when Permanent Device Loss (PDL) and All Paths Down (APD) situations occur and you can enable VM monitoring.

The following tasks are available:

Respond to Host Failure

You can set specific responses to host failures that occur in your vSphere HA cluster.

This page is editable only if you have activated vSphere HA.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Failures and Responses** and then expand **Host Failure Response**.
5. Select from the following configuration options.

Option	Description
Failure Response	If you select **Disabled**, this setting turns off host monitoring and VMs are not restarted when host failures occur. If **Restart VMs** is selected, VMs are failed over based on their restart priority when a host fails.
Default VM Restart Priority	The restart priority determines the order in which virtual machines are restarted when the host fails. Higher priority virtual machines are started first. If multiple hosts fail, all virtual machines are migrated from the first host in order of priority, then all virtual machines from the second host in order of priority, and so on.
VM Restart Priority Condition	A specific condition must be selected as well as a delay after that condition has been met, before vSphere HA is allowed to continue to the next VM restart priority.

6. Click **OK**.

Your settings for the host failure response take effect.

Respond to Host Isolation

You can set specific responses to host isolation that occurs in your vSphere HA cluster.

This page is editable only if you have activated vSphere HA.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Failures and Responses** and expand **Response for Host Isolation**.
5. To configure the host isolation response, select **Disabled**, **Shut down and restart VMs**, or **Power off and restart VMs**.
6. Click **OK**.

Your setting for the host isolation response takes effect.

Configure VMCP Responses

Configure the response that VM Component Protection (VMCP) makes when a datastore encounters a PDL or APD failure.

This page is editable only if you have activated vSphere HA.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Failures and Responses**, and expand either **Datastore with PDL** or **Datastore with APD** .
5. If you clicked **Datastore with PDL**, you can set the VMCP failure response for this type of issue, either **Disabled**, **Issue Events**, or **Power off and restart VMs**.
6. If you clicked **Datastore with APD**, you can set the VMCP failure response for this type of issue, either **Disabled**, **Issue Events**, **Power off and restart VMs--Conservative restart policy**, or **Power off and restart VMs--Aggressive restart policy**. You can also set **Response recovery**, which is the number of minutes that VMCP waits before taking action.
7. Click **OK**.

Your settings for the VMCP failure response take effect.

Enable VM Monitoring

You can turn on VM and Application Monitoring and also set the monitoring sensitivity for your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Failures and Responses** and expand **VM Monitoring**.
5. Select **VM Monitoring** and **Application Monitoring**.
   These settings turn on VMware Tools heartbeats and application heartbeats, respectively.

6. To set the heartbeat monitoring sensitivity, move the slider between **Low** and **High** or select **Custom** to provide custom settings.
7. Click **OK**.

Your monitoring settings take effect.

Configure Proactive HA

You can configure how Proactive HA responds when a provider has notified its health degradation to vCenter, indicating a partial failure of that host.

This page is editable only if you have enabled vSphere DRS.

1. In the vSphere Client, browse to the Proactive HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Select **Turn on Proactive HA**.
5. Click **Proactive HA Failures and Responses**.
6. Select from the following configuration options.

Option	Description
Automation Level	Determine whether host quarantine or maintenance mode and VM migrations are recommendations or automatic. • **Manual**. vCenter Server suggests migration recommendations for virtual machines. • **Automated**. Virtual machines are migrated to healthy hosts and degraded hosts are entered into quarantine or maintenance mode depending on the configured Proactive HA automation level.
Remediation	Determine what happens to partially degraded hosts. • **Quarantine mode for all failures**. Balances performance and availability, by avoiding the usage of partially degraded hosts provided that virtual machine performance is unaffected. • **Quarantine mode for moderate and Maintenance mode for severe failure (Mixed)**. Balances performance and availability, by avoiding the usage of moderately degraded hosts provided that virtual machine performance is unaffected. Ensures that virtual machines do not run on severely failed hosts. • **Maintenance mode for all failures**. Ensures that virtual machines do not run on partially failed hosts. `Host.Config.Quarantine` and `Host.Config.Maintenance` privileges are required to put hosts in Quarantine mode and Maintenance mode, respectively.

To enable Proactive HA providers for this cluster, select the check boxes. Providers appear when their corresponding vSphere Client plugin has been installed and the providers monitor every host in the cluster. To view or edit the failure conditions supported by the provider, click the edit link.

7. Click **OK**.

Configure Admission Control

After you create a cluster, you can configure admission control to specify whether virtual machines can be started if they violate availability constraints. The cluster reserves resources so that failover can occur for all running virtual machines on the specified number of hosts.

The Admission Control page appears only if you activated vSphere HA.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Admission Control** to display the configuration options.
5. Select a number for the **Host failures cluster tolerates**. This is the maximum number of host failures that the cluster can recover from or guarantees failover for.
6. Select an option for **Define host failover capacity by**.

Option	Description
Cluster resource percentage	Specify a percentage of the cluster's CPU and memory resources to reserve as spare capacity to support failovers.
Slot Policy (powered-on VMs)	Select a slot size policy that covers all powered on VMs or is a fixed size. You can also calculate how many VMs require multiple slots.
Dedicated failover hosts	Select hosts to use for failover actions. Failovers can still occur on other hosts in the cluster if a default failover host does not have enough resources.
Disabled	Select this option to deactivate admission control and allow virtual machine power ons that violate availability constraints.

7. Set the percentage for the **Performance degradation VMs tolerate**.

   This setting determines what percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure.
8. Click **OK**.

Your admission control settings take effect.

Configure Heartbeat Datastores

vSphere HA uses datastore heartbeating to distinguish between hosts that have failed and hosts that reside on a network partition. With datastore heartbeating, vSphere HA can monitor hosts when a management network partition occurs and continue to respond to failures.

You can specify the datastores that you want to be used for datastore heartbeating.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Heartbeat Datastores** to display the configuration options for datastore heartbeating.
5. To instruct vSphere HA about how to select the datastores and how to treat your preferences, select from the following options.

Table 346:

Datastore Heartbeating Options
Automatically select datastores accessible from the host
Use datastores only from the specified list
Use datastores from the specified list and complement automatically if needed

6. In the Available heartbeat datastores pane, select the datastores that you want to use for heartbeating.
   The listed datastores are shared by more than one host in the vSphere HA cluster. When a datastore is selected, the lower pane displays all the hosts in the vSphere HA cluster that can access it.
7. Click **OK**.

Set Advanced Options

To customize vSphere HA behavior, set advanced vSphere HA options.

Verify that you have cluster administrator privileges.

Note: Because these options affect the functioning of vSphere HA, change them with caution.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Select **vSphere Availability** and click **Edit**.
4. Click **Advanced Options**.
5. Click **Add** and type the name of the advanced option in the text box.
   You can set the value of the option in the text box in the Value column.
6. Repeat step 5 for each new option that you want to add and click **OK**.

The cluster uses the options that you added or modified.

Once you have set an advanced vSphere HA option, it persists until you do one the following:

- Using the vSphere Client, reset its value to the default value.
- Manually edit or delete the option from the fdm.cfg file on all hosts in the cluster.

vSphere HA Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

Table 347: vSphere HA Advanced Options

Option	Description
das.isolationaddress[...]	Sets the address to ping to determine if a host is isolated from the network. This address is pinged only when heartbeats are not received from any other host in the cluster. If not specified, the default gateway of the management network is used. This default gateway has to be a reliable address that is available, so that the host can determine if it is isolated from the network. You can specify multiple isolation addresses (up to 10) for the cluster: das.isolationAddressX, where X = 0-9. Typically you should specify one per management network. Specifying too many addresses makes isolation detection take too long.
das.usedefaultisolationaddress	By default, vSphere HA uses the default gateway of the console network as an isolation address. This option specifies whether or not this default is used (true|false).
das.isolationshutdowntimeout	The period of time the system waits for a virtual machine to shut down before powering it off. This only applies if the host's isolation response is Shut down VM. Default value is 300 seconds.
das.slotmeminmb	Defines the maximum bound on the memory slot size. If this option is used, the slot size is the smaller of this value or the maximum memory reservation plus memory overhead of any powered-on virtual machine in the cluster.
das.slotcpuinmhz	Defines the maximum bound on the CPU slot size. If this option is used, the slot size is the smaller of this value or the maximum CPU reservation of any powered-on virtual machine in the cluster.
das.vmmemoryminmb	Defines the default memory resource value assigned to a virtual machine if its memory reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default is 0 MB.
das.vmcpuminmhz	Defines the default CPU resource value assigned to a virtual machine if its CPU reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default is 32MHz.
das.iostatsinterval	Changes the default I/O stats interval for VM Monitoring sensitivity. The default is 120 (seconds). Can be set to any value greater than, or equal to 0. Setting to 0 deactivates the check. **Note:** Values of less than 50 are not recommended since smaller values can result in vSphere HA unexpectedly resetting a virtual machine.
das.ignoreinsufficienthbdatastore	Deactivates configuration issues created if the host does not have sufficient heartbeat datastores for vSphere HA. Default value is false.

Option	Description
das.heartbeatdsperhost	Changes the number of heartbeat datastores required. Valid values can range from 2-5 and the default is 2.
das.config.fdm.isolationPolicyDelaySec	The number of seconds system waits before executing the isolation policy once it is determined that a host is isolated. The minimum value is 30. If set to a value less than 30, the delay will be 30 seconds.
das.respectvmvmantiaffinityrules	Determines if vSphere HA enforces VM-VM anti-affinity rules. The default value is "true" and rules are enforced even if vSphere DRS is not activated. In this case, vSphere HA does not fail over a virtual machine if doing so violates a rule, but it issues an event reporting there are insufficient resources to perform the failover. This option can also be set to "false", whereby the rules are not enforced. See *vSphere Resource Management* for more information on anti-affinity rules.
das.maxresets	The maximum number of reset attempts made by VMCP. If a reset operation on a virtual machine affected by an APD situation fails, VMCP retries the reset this many times before giving up
das.maxterminates	The maximum number of retries made by VMCP for virtual machine termination.
das.terminateretryintervalsec	If VMCP fails to terminate a virtual machine, this is the number of seconds the system waits before it retries a terminate attempt
das.config.fdm.reportfailoverfailevent	When set to 1, activates generation of a detailed per-VM event when an attempt by vSphere HA to restart a virtual machine is unsuccessful. Default value is 0. In versions earlier than vSphere 6.0, this event is generated by default.
vpxd.das.completemetadataupdateintervalsec	The period of time (seconds) after a VM-Host affinity rule is set during which vSphere HA can restart a VM in a DRS-deactivated cluster, overriding the rule. Default value is 300 seconds.
das.config.fdm.memReservationMB	By default vSphere HA agents run with a configured memory limit of 250 MB. A host might not allow this reservation if it runs out of reservable capacity. You can use this advanced option to lower the memory limit to avoid this issue. Only integers greater than 100, which is the minimum value, can be specified. Conversely, to prevent problems during primary agent elections in a large cluster (containing 6,000 to 8,000 VMs) you should raise this limit to 325 MB. **Note:** Once this limit is changed, for all hosts in the cluster you must run the Reconfigure HA task. Also, when a new host is added to the cluster or an existing host is rebooted, this task should be performed on those hosts in order to update this memory setting.
das.reregisterrestartdisabledvms	When vSphere HA is deactivated on a specific VM this option ensures that the VM is registered on another host after a failure. This allows you to power-on that VM without needing to re-register it manually. **Note:** When this option is used, vSphere HA does not power on the VM, but only registers it.

Option	Description
das.respectvmhostsoftaffinityrules	Determines if vSphere HA restarts a respective VM on a host that belongs to the same VM-Host group. If no such host is available or if the value of this option is set to “false”, vSphere HA restarts the VM on any available host in the cluster. In vSphere 6.5, the default value is "true". This value might not be visibly defined in the advanced HA options of the cluster. If you want to deactivate the option, you must manually set this option as "false" in the advanced HA options for the cluster.

Note: If you change the value of any of the following advanced options, you must deactivate and then re-activate vSphere HA before your changes take effect.

- das.isolationaddress[...]
- das.usedefaultisolationaddress
- das.isolationshutdowntimeout

Customize an Individual Virtual Machine

Each virtual machine in a vSphere HA cluster is assigned the cluster default settings for VM Restart Priority, Host Isolation Response, VM Component Protection, and VM Monitoring. You can specify specific behavior for each virtual machine by changing these defaults. If the virtual machine leaves the cluster, these settings are lost.

1. In the vSphere Client, browse to the vSphere HA cluster.
2. Click the **Configure** tab.
3. Under Configuration, select **VM Overrides** and click **Add**.
4. Use the **+** button to select virtual machines to which to apply the overrides.
5. Click **OK**.
6. Optional: You can change other settings, such as the **Automation level**, **VM restart priority**, **Response for Host Isolation**, VMCP settings,**VM Monitoring**, or **VM monitoring sensitivity** settings.

   Note: You can view the cluster defaults for these settings by first expanding **Relevant Cluster Settings** and then expanding **vSphere HA**.
7. Click **OK**.

The virtual machine’s behavior now differs from the cluster defaults for each setting that you changed.

Best Practices for VMware vSphere® High Availability Clusters

To ensure optimal vSphere HA cluster performance, you must follow certain best practices. This section highlights some of the key best practices for a vSphere HA cluster.

You can also refer to the *vSphere High Availability Deployment Best Practices* publication for further discussion.

Best Practices for Networking

Observe the following best practices for the configuration of host NICs and network topology for vSphere HA. Best Practices include recommendations for your ESXi hosts, and for cabling, switches, routers, and firewalls.

Network Configuration and Maintenance

The following network maintenance suggestions can help you avoid the accidental detection of failed hosts and network isolation because of dropped vSphere HA heartbeats.

- When changing the networks that your clustered ESXi hosts are on, suspend the Host Monitoring feature. Changing your network hardware or networking settings can interrupt the heartbeats that vSphere HA uses to detect host failures, which might result in unwanted attempts to fail over virtual machines.
- When you change the networking configuration on the ESXi hosts themselves, for example, adding port groups, or removing vSwitches, suspend Host Monitoring. After you have made the networking configuration changes, you must reconfigure vSphere HA on all hosts in the cluster, which causes the network information to be reinspected. Then re-enable Host Monitoring.

Note: Because networking is a vital component of vSphere HA, if network maintenance must be performed inform the vSphere HA administrator.

Networks Used for vSphere HA Communications

To identify which network operations might disrupt the functioning of vSphere HA, you must know which management networks are being used for heart beating and other vSphere HA communications.

- On legacy ESX hosts in the cluster, vSphere HA communications travel over all networks that are designated as service console networks. VMkernel networks are not used by these hosts for vSphere HA communications. To contain vSphere HA traffic to a subset of the ESX console networks, use the allowedNetworks advanced option.
- On ESXi hosts in the cluster, vSphere HA communications, by default, travel over VMkernel networks. With an ESXi host, if you want to use a network other than the one vCenter Server uses to communicate with the host for vSphere HA, you must explicitly enable the **Management traffic** check box.

To keep vSphere HA agent traffic on the networks you have specified, configure hosts so vmkNICs used by vSphere HA do not share subnets with vmkNICs used for other purposes. vSphere HA agents send packets using any pNIC that is associated with a given subnet when there is also at least one vmkNIC configured for vSphere HA management traffic. Therefore, to ensure network flow separation, the vmkNICs used by vSphere HA and by other features must be on different subnets.

Network Isolation Addresses

A network isolation address is an IP address that is pinged to determine whether a host is isolated from the network. This address is pinged only when a host has stopped receiving heartbeats from all other hosts in the cluster. If a host can ping its network isolation address, the host is not network isolated, and the other hosts in the cluster have either failed or are network partitioned. However, if the host cannot ping its isolation address, it is likely that the host has become isolated from the network and no failover action is taken.

By default, the network isolation address is the default gateway for the host. Only one default gateway is specified, regardless of how many management networks have been defined. Use the das.isolationaddress[...] advanced option to add isolation addresses for additional networks. See vSphere HA Advanced Options.

Network Path Redundancy

Network path redundancy between cluster nodes is important for vSphere HA reliability. A single management network ends up being a single point of failure and can result in failovers although only the network has failed. If you have only one management network, any failure between the host and the cluster can cause an unnecessary (or false) failover activity if heartbeat datastore connectivity is not retained during the networking failure. Possible failures include NIC failures, network cable failures, network cable removal, and switch resets. Consider these possible sources of failure between hosts and try to minimize them, typically by providing network redundancy.

The first way you can implement network redundancy is at the NIC level with NIC teaming. Using a team of two NICs connected to separate physical switches improves the reliability of a management network. Because servers connected

through two NICs (and through separate switches) have two independent paths for sending and receiving heartbeats, the cluster is more resilient. To configure a NIC team for the management network, configure the vNICs in vSwitch configuration for Active or Standby configuration. The recommended parameter settings for the vNICs are:

- Default load balancing = route based on originating port ID
- Failback = No

After you have added a NIC to a host in your vSphere HA cluster, you must reconfigure vSphere HA on that host.

In most implementations, NIC teaming provides sufficient heartbeat redundancy, but as an alternative you can create a second management network connection attached to a separate virtual switch. Redundant management networking allows the reliable detection of failures and prevents isolation or partition conditions from occurring, because heartbeats can be sent over multiple networks. The original management network connection is used for network and management purposes. When the second management network connection is created, vSphere HA sends heartbeats over both management network connections. If one path fails, vSphere HA still sends and receives heartbeats over the other path.

Note: Configure the fewest possible number of hardware segments between the servers in a cluster. The goal being to limit single points of failure. Also, routes with too many hops can cause networking packet delays for heartbeats, and increase the possible points of failure.

Using IPv6 Network Configurations

Only one IPv6 address can be assigned to a given network interface used by your vSphere HA cluster. Assigning multiple IP addresses increases the number of heartbeat messages sent by the cluster's primary host with no corresponding benefit.

Best Practices for Interoperability

Observe the following best practices for allowing interoperability between vSphere HA and other features.

vSphere HA and Storage vMotion Interoperability in a Mixed Cluster

In clusters where ESXi 5.x hosts and ESX/ ESXi 4.1 or earlier hosts are present and where Storage vMotion is used extensively or Storage DRS is activated, do not deploy vSphere HA. vSphere HA might respond to a host failure by restarting a virtual machine on a host with an ESXi version different from the one on which the virtual machine was running before the failure. A problem can occur if, at the time of failure, the virtual machine was involved in a Storage vMotion action on an ESXi 5.x host, and vSphere HA restarts the virtual machine on a host with a version earlier than ESXi 5.0. While the virtual machine might power-on, any subsequent attempts at snapshot operations might corrupt the vdisk state and leave the virtual machine unusable.

Using Auto Deploy with vSphere HA

You can use vSphere HA and Auto Deploy together to improve the availability of your virtual machines. Auto Deploy provisions hosts when they power-on and you can also configure it to install the vSphere HA agent on hosts during the boot process. See the Auto Deploy documentation included in vSphere Installation and Setup for details.

Upgrading Hosts in a Cluster Using vSAN

If you are upgrading the ESXi hosts in your vSphere HA cluster to version 5.5 or later, and you also plan to use vSAN, follow this process.

1. Upgrade all of the hosts.
2. Deactivate vSphere HA.
3. Activate vSAN.
4. Re-activate vSphere HA.

Best Practices for Cluster Monitoring

Observe the following best practices for monitoring the status and validity of your vSphere HA cluster.

Setting Alarms to Monitor Cluster Changes

When vSphere HA or Fault Tolerance take action to maintain availability, for example, a virtual machine failover, you can be notified about such changes. Configure alarms in vCenter Server to be triggered when these actions occur, and have alerts, such as emails, sent to a specified set of administrators.

Several default vSphere HA alarms are available.

- Insufficient failover resources (a cluster alarm)
- Cannot find primary (a cluster alarm)
- Failover in progress (a cluster alarm)
- Host HA status (a host alarm)
- VM monitoring error (a virtual machine alarm)
- VM monitoring action (a virtual machine alarm)
- Failover failed (a virtual machine alarm)

Note: The default alarms include the feature name, vSphere HA.

Change in behavior for HA VIBs

In vSphere 7.0, it is possible the HA VIBs might be removed in some cases when HA is activated on a Lifecycle Managed (vLCM) cluster. In previous releases, vCenter would not attempt to remove HA VIBs from ESXi hosts.

This situation can occur only on vLCM clusters with vSphere HA activated. When a vLCM **Remediate** operation occurs (either as a user-initiated operation or an API invocation) after vSphere HA is deactivated on the cluster, the vSphere HA VIBs might be removed as a consequence.

Note: This change in behavior is harmless because vCenter pushes the required vSphere HA VIBs when HA is activated again.

Providing Fault Tolerance for Virtual Machines

You can use vSphere Fault Tolerance for your virtual machines to ensure continuity with higher levels of availability and data protection.

Fault Tolerance is built on the ESXi host platform, and it provides availability by having identical virtual machines run on separate hosts.

To obtain the optimal results from Fault Tolerance you must be familiar with how it works, how to enable it for your cluster, virtual machines and the best practices for its usage.

How Fault Tolerance Works

You can use vSphere Fault Tolerance (FT) for most mission critical virtual machines. FT provides continuous availability for such a virtual machine by creating and maintaining another VM that is identical and continuously available to replace it in the event of a failover situation.

The protected virtual machine is called the Primary VM. The duplicate virtual machine, the Secondary VM, is created and runs on another host. The primary VM is continuously replicated to the secondary VM so that the secondary VM can take over at any point, thereby providing Fault Tolerant protection.

The Primary and Secondary VMs continuously monitor the status of one another to ensure that Fault Tolerance is maintained. A transparent failover occurs if the host running the Primary VM fails, or encounters an uncorrectable

hardware error in the memory of the Primary VM, in which case the Secondary VM is immediately activated to replace the Primary VM. A new Secondary VM is started and Fault Tolerance redundancy is reestablished automatically. If the host running the Secondary VM fails, it is also immediately replaced. In either case, users experience no interruption in service and no loss of data.

A fault tolerant virtual machine and its secondary copy are not allowed to run on the same host. This restriction ensures that a host failure cannot result in the loss of both VMs.

Note: You can also use VM-Host affinity rules to dictate which hosts designated virtual machines can run on. If you use these rules, be aware that for any Primary VM that is affected by such a rule, its associated Secondary VM is also affected by that rule. For more information about affinity rules, see the vSphere Resource Management documentation.

Fault Tolerance avoids "split-brain" situations, which can lead to two active copies of a virtual machine after recovery from a failure. Atomic file locking on shared storage is used to coordinate failover so that only one side continues running as the Primary VM and a new Secondary VM is respawned automatically.

vSphere Fault Tolerance can accommodate symmetric multiprocessor (SMP) virtual machines with up to 8 vCPUs.

Fault Tolerance Use Cases

Several typical situations can benefit from the use of vSphere Fault Tolerance.

Fault Tolerance provides a higher level of business continuity than vSphere HA. When a Secondary VM is called upon to replace its Primary VM counterpart, the Secondary VM immediately takes over the Primary VM's role with the entire state of the virtual machine preserved. Applications are already running, and data stored in memory does not need to be reentered or reloaded. Failover provided by vSphere HA restarts the virtual machines affected by a failure.

This higher level of continuity and the added protection of state information and data informs the scenarios when you might want to deploy Fault Tolerance.

- Applications which must always be available, especially applications that have long-lasting client connections that users want to maintain during hardware failure.
- Custom applications that have no other way of doing clustering.
- Cases where high availability might be provided through custom clustering solutions, which are too complicated to configure and maintain.

Another key use case for protecting a virtual machine with Fault Tolerance can be described as On-Demand Fault Tolerance. In this case, a virtual machine is adequately protected with vSphere HA during normal operation. During certain critical periods, you might want to enhance the protection of the virtual machine. For example, you might be running a quarter-end report which, if interrupted, might delay the availability of critical information. With vSphere Fault Tolerance, you can protect this virtual machine before running this report and then turn off or suspend Fault Tolerance after the report has been produced. You can use On-Demand Fault Tolerance to protect the virtual machine during a critical time period and return the resources to normal during non-critical operation.

Fault Tolerance Requirements, Limits, and Licensing

Before using vSphere Fault Tolerance (FT), consider the high-level requirements, limits, and licensing that apply to this feature.

Requirements

The following CPU and networking requirements apply to FT.

CPUs that are used in host machines for fault tolerant VMs must be compatible with vSphere vMotion. Also, CPUs that support Hardware MMU virtualization (Intel EPT or AMD RVI) are required. The following CPUs are supported.

- Intel Sandy Bridge or later. Avoton is not supported.

- AMD Bulldozer or later.

Use a 10-Gbit logging network for FT and verify that the network is low latency. A dedicated FT network is highly recommended.

Limits

In a cluster configured to use Fault Tolerance, two limits are enforced independently.

das.maxftvmsperhost	The maximum number of fault tolerant VMs allowed on a host in the cluster. The default value is 4. There is no FT VMs per host maximum, you can use larger numbers if the workload performs well in FT VMs. You can deactivate checking by setting the value to `0`.
das.maxftvcpusperhost	The maximum number of vCPUs aggregated across all fault tolerant VMs on a host. The default value is 8. There is no FT vCPU per host maximum, you can use larger numbers if the workload performs well. You can deactivate checking by setting the value to `0`.

Licensing

The number of vCPUs supported by a single fault tolerant VM is limited by the level of licensing that you have purchased for vSphere. Fault Tolerance is supported as follows:

- vSphere Standard and Enterprise. Allows up to 2 vCPUs
- vSphere Enterprise Plus. Allows up to 8 vCPUs

Note: FT is supported in vSphere Standard, vSphere Enterprise and vSphere Enterprise Plus Editions.

Fault Tolerance Interoperability

Before configuring vSphere Fault Tolerance, you must be aware of the features and products Fault Tolerance cannot interoperate with.

vSphere Features Not Supported with Fault Tolerance

When configuring your cluster, you should be aware that not all vSphere features can interoperate with Fault Tolerance.

The following vSphere features are not supported for fault tolerant virtual machines.

Note: Before vSphere 7.0 Update 2, vSphere Virtual Machine Encryption was not supported with FT.

- Snapshots. Snapshots must be removed or committed before Fault Tolerance can be enabled on a virtual machine. In addition, it is not possible to take snapshots of virtual machines on which Fault Tolerance is enabled.
  Note: Disk-only snapshots created for vStorage APIs - Data Protection (VADP) backups are supported with Fault Tolerance. However, legacy FT does not support VADP.
- Storage vMotion. You cannot invoke Storage vMotion for virtual machines with Fault Tolerance turned on. To migrate the storage, you should temporarily turn off Fault Tolerance, and perform the storage vMotion action. When this is complete, you can turn Fault Tolerance back on.
- Linked clones. You cannot use Fault Tolerance on a virtual machine that is a linked clone, nor can you create a linked clone from an FT-enabled virtual machine.
- Virtual Volume datastores.
- Storage-based policy management. Storage policies are supported for vSAN storage.
- I/O filters.
- VBS enabled VMs.

Features and Devices Incompatible with Fault Tolerance

Not all third party devices, features, or products can interoperate with Fault Tolerance.

For a virtual machine to be compatible with Fault Tolerance, the Virtual Machine must not use the following features or devices.

Table 348: Features and Devices Incompatible with Fault Tolerance and Corrective Actions

Incompatible Feature or Device	Corrective Action
Physical Raw Disk mapping (RDM).	With legacy FT you can reconfigure virtual machines with physical RDM-backed virtual devices to use virtual RDMs instead.
CD-ROM or floppy virtual devices backed by a physical or remote device.	Remove the CD-ROM or floppy virtual device or reconfigure the backing with an ISO installed on shared storage.
USB and sound devices.	Remove these devices from the virtual machine.
N_Port ID Virtualization (NPIV).	Deactivate the NPIV configuration of the virtual machine.
NIC passthrough.	This feature is not supported by Fault Tolerance so it must be turned off.
Hot-plugging devices.	The hot plug feature is automatically deactivated for fault tolerant virtual machines. To hot plug devices (either adding or removing), you must momentarily turn off Fault Tolerance, perform the hot plug, and then turn on Fault Tolerance. **Note:** When using Fault Tolerance, changing the settings of a virtual network card while a virtual machine is running is a hot-plug operation, since it requires "unplugging" the network card and then "plugging" it in again. For example, with a virtual network card for a running virtual machine, if you change the network that the virtual NIC is connected to, FT must be turned off first.
Serial or parallel ports	Remove these devices from the virtual machine.
Video devices that have 3D activated.	Fault Tolerance does not support video devices that have 3D activated.
Virtual Machine Communication Interface (VMCI)	Not supported by Fault Tolerance.
2TB+ VMDK	Fault Tolerance is not supported with a 2TB+ VMDK.

Using Fault Tolerance with DRS

You can use vSphere Fault Tolerance with vSphere Distributed Resource Scheduler (DRS).

FT VMs do not require EVC to support DRS. You can use FT with DRS on vSphere 6.5 and 6.0 hosts that are managed by a vSphere 6.7 or higher VC.

Note: vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See *vSphere Cluster Services (vCLS)* in *vSphere Resource Management* for more information.

Preparing Your Cluster and Hosts for Fault Tolerance

To enable vSphere Fault Tolerance for your cluster, you must meet the feature's prerequisites and you must perform certain configuration steps on your hosts. After those steps are accomplished and your cluster has been created, you can also check that your configuration complies with the requirements for enabling Fault Tolerance.

The tasks you should complete before attempting to set up Fault Tolerance for your cluster include the following:

- Ensure that your cluster, hosts, and virtual machines meet the requirements outlined in the Fault Tolerance checklist.
- Configure networking for each host.
- Create the vSphere HA cluster, add hosts, and check compliance.

After your cluster and hosts are prepared for Fault Tolerance, you are ready to turn on Fault Tolerance for your virtual machines. See Turn On Fault Tolerance.

Fault Tolerance Checklist

The following checklist contains cluster, host, and virtual machine requirements that you need to be aware of before using vSphere Fault Tolerance.

Review this list before setting up Fault Tolerance.

Note: The failover of fault tolerant virtual machines is independent of vCenter Server, but you must use vCenter Server to set up your Fault Tolerance clusters.

Cluster Requirements for Fault Tolerance

You must meet the following cluster requirements before you use Fault Tolerance.

- Fault Tolerance logging and VMotion networking configured. See Configure Networking for Host Machines.
- vSphere HA cluster created and enabled. See Creating a vSphere HA Cluster. vSphere HA must be enabled before you can power on fault tolerant virtual machines or add a host to a cluster that already supports fault tolerant virtual machines.

Host Requirements for Fault Tolerance

You must meet the following host requirements before you use Fault Tolerance.

- Hosts must use supported processors.
- Hosts must be licensed for Fault Tolerance.
- Hosts must be certified for Fault Tolerance. See http://www.vmware.com/resources/compatibility/search.php and select **Search by Fault Tolerant Compatible Sets** to determine if your hosts are certified.
- The configuration for each host must have Hardware Virtualization (HV) enabled in the BIOS.

Note: VMware recommends that the hosts you use to support FT VMs have their BIOS power management settings turned to "Maximum performance" or "OS-managed performance".

To confirm the compatibility of the hosts in the cluster to support Fault Tolerance, you can also run profile compliance checks as described in Create Cluster and Check Compliance.

Virtual Machine Requirements for Fault Tolerance

You must meet the following virtual machine requirements before you use Fault Tolerance.

- No unsupported devices attached to the virtual machine. See Fault Tolerance Interoperability.
- Incompatible features must not be running with the fault tolerant virtual machines. See Fault Tolerance Interoperability.
- Virtual machine files (except for the VMDK files) must be stored on shared storage. Acceptable shared storage solutions include Fibre Channel, (hardware and software) iSCSI, vSAN, NFS, and NAS.

Other Configuration Recommendations

You should also observe the following guidelines when configuring Fault Tolerance.

- If you are using NFS to access shared storage, use dedicated NAS hardware with at least a 1Gbit NIC to obtain the network performance required for Fault Tolerance to work properly.

- The memory reservation of a fault tolerant virtual machine is set to the VM's memory size when Fault Tolerance is turned on. Ensure that a resource pool containing fault tolerant VMs has memory resources above the memory size of the virtual machines. Without this excess in the resource pool, there might not be any memory available to use as overhead memory.
- To ensure redundancy and maximum Fault Tolerance protection, you should have a minimum of three hosts in the cluster. In a failover situation, this provides a host that can accommodate the new Secondary VM that is created.

Configure Networking for Host Machines

On each host that you want to add to a vSphere HA cluster, you must configure two different networking switches (vMotion and FT logging) so that the host can support vSphere Fault Tolerance.

Multiple gigabit Network Interface Cards (NICs) are required. For each host supporting Fault Tolerance, a minimum of two physical NICs is recommended. For example, you need one dedicated to Fault Tolerance logging and one dedicated to vMotion. Use three or more NICs to ensure availability.

To set up Fault Tolerance for a host, you must complete this procedure for each port group option (vMotion and FT logging) to ensure that sufficient bandwidth is available for Fault Tolerance logging. Select one option, finish this procedure, and repeat the procedure a second time, selecting the other port group option.

1. In the vSphere Client, browse to the host.
2. Click the **Configure** tab and click **Networking**.
3. Select **VMkernel adapters**.
4. Click the **Add Networking** icon.
5. Provide appropriate information for your connection type.
6. Click **Finish**.

After you create both a vMotion and Fault Tolerance logging virtual switch, you can create other virtual switches, as needed. Add the host to the cluster and complete any steps needed to turn on Fault Tolerance.
Note: If you configure networking to support FT but subsequently suspend the Fault Tolerance logging port, pairs of fault tolerant virtual machines that are powered on remain powered on. If a failover situation occurs, when the Primary VM is replaced by its Secondary VM a new Secondary VM is not started, causing the new Primary VM to run in a Not Protected state.

Create Cluster and Check Compliance

vSphere Fault Tolerance is used in the context of a vSphere HA cluster. After you configure networking on each host, create the vSphere HA cluster and add the hosts to it. You can check to see whether the cluster is configured correctly and complies with the requirements for the enablement of Fault Tolerance.

1. In the vSphere Client, browse to the cluster.
2. Click the **Monitor** tab and click **Profile Compliance**.
3. Click **Check Compliance Now** to run the compliance tests.

The results of the compliance test appear, and the compliance or noncompliance of each host is shown.

Using Fault Tolerance

After you have taken all of the required steps for activating vSphere Fault Tolerance for your cluster, you can use the feature by turning it on for individual virtual machines.

Before Fault Tolerance can be turned on, validation checks are performed on a virtual machine.

After these checks are passed and you turn on vSphere Fault Tolerance for a virtual machine, new options are added to the Fault Tolerance section of its context menu. These include turning off or deactivating Fault Tolerance, migrating the Secondary VM, testing failover, and testing restart of the Secondary VM.

Validation Checks for Turning On Fault Tolerance

If the option to turn on Fault Tolerance is available, this task still must be validated and can fail if certain requirements are not met.

Several validation checks are performed on a virtual machine before Fault Tolerance can be turned on.

- SSL certificate checking must be activated in the vCenter Server settings.
- The host must be in a vSphere HA cluster or a mixed vSphere HA and DRS cluster.
- The host must have ESXi 6.x or greater installed.
- The virtual machine must not have snapshots.
- The virtual machine must not be a template.
- The virtual machine must not have vSphere HA deactivated.
- The virtual machine must not have a video device with 3D activated.

Checks for Powered-On Virtual Machines

Several additional validation checks are performed for powered-on virtual machines (or those that are in the process of being powered on).

- The BIOS of the hosts where the fault tolerant virtual machines reside must have Hardware Virtualization (HV) activated.
- The host that supports the Primary VM must have a processor that supports Fault Tolerance.
- Your hardware should be certified as compatible with Fault Tolerance. To confirm that it is, use the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php and select **Search by Fault Tolerant Compatible Sets**.
- The configuration of the virtual machine must be valid for use with Fault Tolerance (for example, it must not contain any unsupported devices).

Secondary VM Placement

When your effort to turn on Fault Tolerance for a virtual machine passes the validation checks, the Secondary VM is created. The placement and immediate status of the Secondary VM depends upon whether the Primary VM was powered-on or powered-off when you turned on Fault Tolerance.

If the Primary VM is powered on:

- The entire state of the Primary VM is copied and the Secondary VM is created, placed on a separate compatible host, and powered on if it passes admission control.
- The Fault Tolerance Status displayed for the virtual machine is **Protected**.

If the Primary VM is powered off:

- The Secondary VM is immediately created and registered to a host in the cluster (it might be re-registered to a more appropriate host when it is powered on.)
- The Secondary VM is not powered on until after the Primary VM is powered on.
- The Fault Tolerance Status displayed for the virtual machine is **Not Protected, VM not Running**.
- When you attempt to power on the Primary VM after Fault Tolerance has been turned on, the additional validation checks listed above are performed.

  After these checks are passed, the Primary and Secondary VMs are powered on and placed on separate, compatible hosts. The virtual machine's Fault Tolerance Status is tagged as **Protected**.

Turn On Fault Tolerance

You can turn on vSphere Fault Tolerance through the vSphere Client.

The option to turn on Fault Tolerance is unavailable (dimmed) if any of these conditions apply:

- The virtual machine resides on a host that does not have a license for the feature.
- The virtual machine resides on a host that is in maintenance mode or standby mode.
- The virtual machine is disconnected or orphaned (its .vmx file cannot be accessed).
- The user does not have permission to turn the feature on.

When Fault Tolerance is turned on, vCenter Server resets the virtual machine's memory limit and sets the memory reservation to the memory size of the virtual machine. While Fault Tolerance remains turned on, you cannot change the memory reservation, size, limit, number of vCPUs, or shares. You also cannot add or remove disks for the VM. When Fault Tolerance is turned off, any parameters that were changed are not reverted to their original values.
Connect vSphere Client to vCenter Server using an account with cluster administrator permissions.

1. In the vSphere Client, browse to the virtual machine for which you want to turn on Fault Tolerance.
2. Right-click the virtual machine and select **Fault Tolerance** > **Turn On Fault Tolerance**.
3. Click **Yes**.
4. Select a datastore on which to place the Secondary VM configuration files. Then click **Next**.
5. Select a host on which to place the Secondary VM. Then click **Next**.
6. Review your selections and then click **Finish**.

The specified virtual machine is designated as a Primary VM, and a Secondary VM is established on another host. The Primary VM is now fault tolerant.

Note: The VM datastores and memory are replicated during the FT Turn On process. This can take several minutes depending on the size of the replicated data. The VM state does not appear as protected until replication is complete.

Turn Off Fault Tolerance

Turning off vSphere Fault Tolerance deletes the secondary virtual machine, its configuration, and all history.

Use the **Turn Off Fault Tolerance** option if you do not plan to reenable the feature. Otherwise, use the **Suspend Fault Tolerance** option.

Note: If the Secondary VM resides on a host that is in maintenance mode, disconnected, or not responding, you cannot use the **Turn Off Fault Tolerance** option. In this case, you should suspend and resume Fault Tolerance instead.

1. In the vSphere Client, browse to the virtual machine for which you want to turn off Fault Tolerance.
2. Right-click the virtual machine and select **Fault Tolerance** > **Turn Off Fault Tolerance**.
3. Click **Yes**.

Fault Tolerance is turned off for the selected virtual machine. The history and the secondary virtual machine for the selected virtual machine are deleted.

Note: Fault Tolerance cannot be turned off when the secondary VM is in the process of being started. Since this involves syncing up the primary VM's full state to the secondary VM, this process may take longer than expected.

Suspend Fault Tolerance

Suspending vSphere Fault Tolerance for a virtual machine suspends its Fault Tolerance protection, but preserves the Secondary VM, its configuration, and all history. Use this option to resume Fault Tolerance protection in the future.

1. In the vSphere Client, browse to the virtual machine for which you want to suspend Fault Tolerance.
2. Right-click the virtual machine and select **Fault Tolerance** > **Suspend Fault Tolerance**.
3. Click **Yes**.

Fault Tolerance is suspended for the selected virtual machine. Any history and the Secondary VM for the selected virtual machine are preserved and will be used if the feature is resumed.

After you suspend Fault Tolerance, to resume the feature select **Resume Fault Tolerance**.

Migrate Secondary

After vSphere Fault Tolerance is turned on for a Primary VM, you can migrate its associated Secondary VM.

1. In the vSphere Client, browse to the Primary VM for which you want to migrate its Secondary VM.
2. Right-click the virtual machine and select **Fault Tolerance** > **Migrate Secondary**.
3. Complete the options in the Migrate dialog box and confirm the changes that you made.
4. Click **Finish** to apply the changes.

The Secondary VM associated with the selected fault tolerant virtual machine is migrated to the specified host.

Test Failover

You can induce a failover situation for a selected Primary VM to test your Fault Tolerance protection.

This option is unavailable (dimmed) if the virtual machine is powered off.

1. In the vSphere Client, browse to the Primary VM for which you want to test failover.
2. Right-click the virtual machine and select **Fault Tolerance** > **Test Failover**.
3. View details about the failover in the Task Console.

This task induces failure of the Primary VM to ensure that the Secondary VM replaces it. A new Secondary VM is also started placing the Primary VM back in a Protected state.

Test Restart Secondary

You can induce the failure of a Secondary VM to test the Fault Tolerance protection provided for a selected Primary VM.

This option is unavailable (dimmed) if the virtual machine is powered off.

1. In the vSphere Client, browse to the Primary VM for which you want to conduct the test.
2. Right-click the virtual machine and select **Fault Tolerance** > **Test Restart Secondary**.
3. View details about the test in the Task Console.

This task results in the termination of the Secondary VM that provided Fault Tolerance protection for the selected Primary VM. A new Secondary VM is started, placing the Primary VM back in a Protected state.

Upgrade Hosts Used for Fault Tolerance

Use the following procedure to upgrade hosts used for Fault Tolerance.

Verify that you have cluster administrator privileges.

Verify that you have sets of four or more ESXi hosts that are hosting fault tolerant virtual machines that are powered on. If the virtual machines are powered off, the Primary and Secondary VMs can be relocated to hosts with different builds.

Note: This upgrade procedure is for a minimum four-node cluster. The same instructions can be followed for a smaller cluster, though the unprotected interval will be slightly longer.

1. Using vMotion, migrate the fault tolerant virtual machines off of two hosts.
2. Upgrade the two evacuated hosts to the same ESXi build.
3. Suspend Fault Tolerance on the Primary VM.
4. Using vMotion, move the Primary VM for which Fault Tolerance has been suspended to one of the upgraded hosts.
5. Resume Fault Tolerance on the Primary VM that was moved.
6. Repeat 1 to 5 for as many fault tolerant virtual machine pairs as can be accommodated on the upgraded hosts.
7. Using vMotion, redistribute the fault tolerant virtual machines.

All ESXi hosts in a cluster are upgraded.

Activate Fault Tolerance Encryption

You can encrypt Fault Tolerance log traffic.

FT encryption requires SMP-FT. Encryption on Legacy FT (Record-Replay FT) is not supported.

vSphere Fault Tolerance performs frequent checks between a primary VM and secondary VM so that the secondary VM can quickly resume from the last successful checkpoint. The checkpoint contains the VM state that has been modified since the previous checkpoint. You can encrypt Fault Tolerance log traffic.

When you turn on Fault Tolerance, FT encryption is set to **Opportunistic** by default, which means it activates encryption only if both the primary and secondary host are capable of encryption. Follow this procedure if you need to change the FT encryption mode manually.

Note: Fault Tolerance supports vSphere Virtual Machine Encryption with vSphere 7.0 Update 2 and later. In-guest and array-based encryption do not depend on or interfere with VM encryption. Having multiple encryption layers uses additional compute resources, which might impact virtual machine performance. The impact varies with hardware as well as the amount and type of I/O, but overall performance impact is negligible for most workloads. The effectiveness and compatibility of back-end storage features such as deduplication, compression, and replication might also be affected by VM encryption.

1. Select the VM and choose **Edit Settings**.
2. Under **VM Options** select the **Encrypted FT** drop-down menu.
3. Choose one of the following options:

Option	Description
Disabled	Do not turn on encrypted Fault Tolerance logging.
Opportunistic	Turn on encryption only if both sides are capable. A Fault Tolerance VM is allowed to move to an ESXi host which does not support encrypted Fault Tolerance logging.

Option	Description
Required	Choose hosts for Fault Tolerance primary and secondary that both support encrypted FT logging.

Note: While VM encryption is activated, FT encryption mode is set to **Required** by default and cannot be modified.

When FT encryption mode is set to **Required**:

- When you turn on FT, only FT encryption supported hosts are listed for the placement of FT secondary.
- FT failover can only happen on the FT encryption supported hosts.

4. Click **OK**.

Best Practices for Fault Tolerance

To ensure optimal Fault Tolerance results, you should follow certain best practices.

The following recommendations for host and networking configuration can help improve the stability and performance of your cluster.

Host Configuration

Hosts running the Primary and Secondary VMs should operate at approximately the same processor frequencies, otherwise the Secondary VM might be restarted more frequently. Platform power management features that do not adjust based on workload (for example, power capping and enforced low frequency modes to save power) can cause processor frequencies to vary greatly. If Secondary VMs are being restarted on a regular basis, deactivate all power management modes on the hosts running fault tolerant virtual machines or ensure that all hosts are running in the same power management modes.

Host Networking Configuration

The following guidelines allow you to configure your host's networking to support Fault Tolerance with different combinations of traffic types (for example, NFS) and numbers of physical NICs.

- Distribute each NIC team over two physical switches ensuring L2 domain continuity for each VLAN between the two physical switches.
- Use deterministic teaming policies to ensure particular traffic types have an affinity to a particular NIC (active/standby) or set of NICs (for example, originating virtual port-id).
- Where active/standby policies are used, pair traffic types to minimize impact in a failover situation where both traffic types will share a vmnic.
- Where active/standby policies are used, configure all the active adapters for a particular traffic type (for example, FT Logging) to the same physical switch. This minimizes the number of network hops and lessens the possibility of oversubscribing the switch to switch links.

Note: FT logging traffic between Primary and Secondary VMs is unencrypted and contains guest network and storage I/O data, as well as the memory contents of the guest operating system. This traffic can include sensitive data such as passwords in plaintext. To avoid such data being divulged, ensure that this network is secured, especially to avoid 'man-in-the-middle' attacks. For example, you could use a private network for FT logging traffic.

Homogeneous Clusters

vSphere Fault Tolerance can function in clusters with nonuniform hosts, but it works best in clusters with compatible nodes. When constructing your cluster, all hosts should have the following configuration:

- Common access to datastores used by the virtual machines.
- The same virtual machine network configuration.
- The same BIOS settings (power management and hyperthreading) for all hosts.

Run **Check Compliance** to identify incompatibilities and to correct them.

Performance

To increase the bandwidth available for the logging traffic between Primary and Secondary VMs use a 10Gbit NIC, and activate the use of jumbo frames.

You can select multiple NICs for the FT logging network. By selecting multiple NICs, you can take advantage of the bandwidth from multiple NICs even if all of the NICs are not dedicated to running FT.

Store ISOs on Shared Storage for Continuous Access

Store ISOs that are accessed by virtual machines with Fault Tolerance activated on shared storage that is accessible to both instances of the fault tolerant virtual machine. If you use this configuration, the CD-ROM in the virtual machine continues operating normally, even when a failover occurs.

Avoid Network Partitions

A network partition occurs when a vSphere HA cluster has a management network failure that isolates some of the hosts from vCenter Server and from one another. See Network Partitions . When a partition occurs, Fault Tolerance protection might be degraded.

In a partitioned vSphere HA cluster using Fault Tolerance, the Primary VM (or its Secondary VM) could end up in a partition managed by a primary host that is not responsible for the virtual machine. When a failover is needed, a Secondary VM is restarted only if the Primary VM was in a partition managed by the primary host responsible for it.

To ensure that your management network is less likely to have a failure that leads to a network partition, follow the recommendations in Best Practices for Networking.

Using vSAN Datastores

vSphere Fault Tolerance can use vSAN datastores, but you must observe the following restrictions:

- A mix of vSAN and other types of datastores is not supported for both Primary VMs and Secondary VMs.
- vSAN metro clusters are not supported with FT.

To increase performance and reliability when using FT with vSAN, the following conditions are also recommended.

- vSAN and FT should use separate networks.
- Keep Primary and Secondary VMs in separate vSAN fault domains.

Legacy Fault Tolerance

Legacy FT VMs can exist only on ESXi hosts that are running on vSphere versions earlier than 6.5.

ESXi hosts prior to version 6.5 supported vSphere Fault Tolerance based on a different technology. If you are using this form of Fault Tolerance and need to continue doing so, we recommend you reserve a vCenter 6.0 instance to manage the pool of pre-6.5 hosts required to run these VMs. vCenter 6.0 was the last version fully capable of managing legacy FT protected VMs. For more information on Legacy Fault Tolerance, see vSphere Availability 6.0 documentation.

Troubleshooting Fault Tolerant Virtual Machines

To maintain a high level of performance and stability for your fault tolerant virtual machines and also to minimize failover rates, you should be aware of certain troubleshooting issues.

The troubleshooting topics discussed focus on problems that you might encounter when using the vSphere Fault Tolerance feature on your virtual machines. The topics also describe how to resolve problems.

You can also see the VMware knowledge base article at http://kb.vmware.com/kb/1033634 to help you troubleshoot Fault Tolerance. This article contains a list of error messages that you might encounter when you attempt to use the feature and, where applicable, advice on how to resolve each error.

Hardware Virtualization Not Enabled

You must enable Hardware Virtualization (HV) before you use vSphere Fault Tolerance.

When you attempt to power on a virtual machine with Fault Tolerance enabled, an error message might appear if you did not enable HV.

This error is often the result of HV not being available on the ESXi server on which you are attempting to power on the virtual machine. HV might not be available either because it is not supported by the ESXi server hardware or because HV is not enabled in the BIOS.

If the ESXi server hardware supports HV, but HV is not currently enabled, enable HV in the BIOS on that server. The process for enabling HV varies among BIOSes. See the documentation for your hosts' BIOSes for details on how to enable HV.

If the ESXi server hardware does not support HV, switch to hardware that uses processors that support Fault Tolerance.

Compatible Hosts Not Available for Secondary VM

If you power on a virtual machine with Fault Tolerance enabled and no compatible hosts are available for its Secondary VM, you might receive an error message.

You might encounter the following error message:

```
Secondary VM could not be powered on as there are no compatible hosts that can accommodate
 it.
```

This can occur for a variety of reasons including that there are no other hosts in the cluster, there are no other hosts with HV enabled, Hardware MMU Virtualization is not supported by host CPUs, data stores are inaccessible, there is no available capacity, or hosts are in maintenance mode.

If there are insufficient hosts, add more hosts to the cluster. If there are hosts in the cluster, ensure they support HV and that HV is enabled. The process for enabling HV varies among BIOSes. See the documentation for your hosts' BIOSes for details on how to enable HV. Check that hosts have sufficient capacity and that they are not in maintenance mode.

Secondary VM on Overcommitted Host Degrades Performance of Primary VM

If a Primary VM appears to be executing slowly, even though its host is lightly loaded and retains idle CPU time, check the host where the Secondary VM is running to see if it is heavily loaded.

When a Secondary VM resides on a host that is heavily loaded, the Secondary VM can affect the performance of the Primary VM.

A Secondary VM running on a host that is overcommitted (for example, with its CPU resources) might not get the same amount of resources as the Primary VM. When this occurs, the Primary VM must slow down to allow the Secondary VM to keep up, effectively reducing its execution speed to the slower speed of the Secondary VM.

If the Secondary VM is on an overcommitted host, you can move the VM to another location without resource contention problems. Or more specifically, do the following:

- For FT networking contention, use vMotion technology to move the Secondary VM to a host with fewer FT VMs contending on the FT network. Verify that the quality of the storage access to the VM is not asymmetric.

- For storage contention problems, turn FT off and on again. When you recreate the Secondary VM, change its datastore to a location with less resource contention and better performance potential.
- To resolve a CPU resources problem, set an explicit CPU reservation for the Primary VM at an MHz value sufficient to run its workload at the desired performance level. This reservation is applied to both the Primary and Secondary VMs, ensuring that both VMs can execute at a specified rate. For guidance in setting this reservation, view the performance graphs of the virtual machine (before Fault Tolerance was enabled) to see how many CPU resources it used under normal conditions.

Increased Network Latency Observed in FT Virtual Machines

If your FT network is not optimally configured, you might experience latency problems with the FT VMs.

FT VMs might see a variable increase in packet latency (on the order of milliseconds). Applications that demand very low network packet latency or jitter (for example, certain real-time applications) might see a degradation in performance.

Some increase in network latency is expected overhead for Fault Tolerance, but certain factors can add to this latency. For example, if the FT network is on a particularly high latency link, this latency is passed on to the applications. Also, if the FT network has insufficient bandwidth (fewer than 10 Gbps), greater latency might occur.

Verify that the FT network has sufficient bandwidth (10 Gbps or more) and uses a low latency link between the Primary VM and Secondary VM. These precautions do not eliminate network latency, but minimize its potential impact.

Some Hosts Are Overloaded with FT Virtual Machines

You might encounter performance problems if your cluster's hosts have an imbalanced distribution of FT VMs.

Some hosts in the cluster might become overloaded with FT VMs, while other hosts might have unused resources.

vSphere DRS does not load balance FT VMs (unless they are using legacy FT). This limitation might result in a cluster where hosts are unevenly distributed with FT VMs.

Manually rebalance the FT VMs across the cluster by using vSphere vMotion. Generally, the fewer FT VMs that are on a host, the better they perform, due to reduced contention for FT network bandwidth and CPU resources.

Losing Access to FT Metadata Datastore

Access to the Fault Tolerance metadata datastore is essential for the proper functioning of an FT VM. Loss of this access can cause a variety of problems.

These problems include the following:

- FT can terminate unexpectedly.
- If both the Primary VM and Secondary VM cannot access the metadata datastore, the VMs might fail unexpectedly. Typically, an unrelated failure that terminates FT must also occur when access to the FT metadata datastore is lost by both VMs. vSphere HA then tries to restart the Primary VM on a host with access to the metadata datastore.
- The VM might stop being recognized as an FT VM by vCenter Server. This failed recognition can allow unsupported operations such as taking snapshots to be performed on the VM and cause problematic behavior.

Lack of access to the Fault Tolerance metadata datastore can lead to the undesirable outcomes in the previous list.

When planning your FT deployment, place the metadata datastore on highly available storage. While FT is running, if you see that the access to the metadata datastore is lost on either the Primary VM or the Secondary VM, promptly address the storage problem before loss of access causes one of the previous problems. If a VM stops being recognized as an FT VM by vCenter Server, do not perform unsupported operations on the VM. Restore access to the metadata datastore. After access is restored for the FT VMs and the refresh period has ended, the VMs are recognizable.

Turning On vSphere FT for Powered-On VM Fails

If you try to turn on vSphere Fault Tolerance for a powered-on VM, this operation can fail.

When you select **Turn On Fault Tolerance** for a powered-on VM, the operation fails and you see an `Unknown error` message.

This operation can fail if the host that the VM is running on has insufficient memory resources to provide fault tolerant protection. vSphere Fault Tolerance automatically tries to allocate a full memory reservation on the host for the VM. Overhead memory is required for fault tolerant VMs and can sometimes expand to 1 to 2 GB. If the powered-on VM is running on a host that has insufficient memory resources to accommodate the full reservation plus the overhead memory, trying to turn on Fault Tolerance fails. Subsequently, the `Unknown error` message is returned.

Choose from these solutions:

- Free up memory resources on the host to accommodate the VM's memory reservation and the added overhead.
- Move the VM to a host with ample free memory resources and try again.

FT Virtual Machines not Placed or Evacuated by vSphere DRS

FT virtual machines in a cluster that is activated with vSphere DRS do not function correctly if Enhanced vMotion Compatibility (EVC) is currently deactivated.

Because EVC is a prerequisite for using DRS with FT VMs, DRS does not place or evacuate them if EVC has been deactivated (even if it is later reactivated).

When EVC is deactivated on a DRS cluster, a VM override that deactivates DRS on an FT VM might be added. Even if EVC is later reactivated, this override is not canceled.

If DRS does not place or evacuate FT VMs in the cluster, check the VMs for a VM override that is deactivating DRS. If you find one, remove the override that is deactivating DRS.

Note: For more information on how to edit or delete VM overrides, see *vSphere Resource Management*.

Fault Tolerant Virtual Machine Failovers

A Primary or Secondary VM can fail over even though its ESXi host has not crashed. In such cases, virtual machine execution is not interrupted, but redundancy is temporarily lost. To avoid this type of failover, be aware of some of the situations when it can occur and take steps to avoid them.

Partial Hardware Failure Related to Storage

This problem can arise when access to storage is slow or down for one of the hosts. When this occurs there are many storage errors listed in the VMkernel log. To resolve this problem you must address your storage-related problems.

Partial Hardware Failure Related to Network

If the logging NIC is not functioning or connections to other hosts through that NIC are down, this can trigger a fault tolerant virtual machine to be failed over so that redundancy can be reestablished. To avoid this problem, dedicate a separate NIC each for vMotion and FT logging traffic and perform vMotion migrations only when the virtual machines are less active.

Insufficient Bandwidth on the Logging NIC Network

This can happen because of too many fault tolerant virtual machines being on a host. To resolve this problem, more broadly distribute pairs of fault tolerant virtual machines across different hosts.

Use a10-Gbit logging network for FT and verify that the network is low latency.

vMotion Failures Due to Virtual Machine Activity Level

If the vMotion migration of a fault tolerant virtual machine fails, the virtual machine might need to be failed over. Usually, this occurs when the virtual machine is too active for the migration to be completed with only minimal disruption to the activity. To avoid this problem, perform vMotion migrations only when the virtual machines are less active.

Too Much Activity on VMFS Volume Can Lead to Virtual Machine Failovers

When a number of file system locking operations, virtual machine power ons, power offs, or vMotion migrations occur on a single VMFS volume, this can trigger fault tolerant virtual machines to be failed over. A symptom that this might be occurring is receiving many warnings about SCSI reservations in the VMkernel log. To resolve this problem, reduce the number of file system operations or ensure that the fault tolerant virtual machine is on a VMFS volume that does not have an abundance of other virtual machines that are regularly being powered on, powered off, or migrated using vMotion.

Lack of File System Space Prevents Secondary VM Startup

Check whether or not your /(root) or /vmfs/*datasource* file systems have available space. These file systems can become full for many reasons, and a lack of space might prevent you from being able to start a new Secondary VM.

vCenter High Availability

vCenter High Availability (vCenter HA) protects vCenter Server against host and hardware failures. The active-passive architecture of the solution can also help you reduce downtime significantly when you patch vCenter Server.

After some network configuration, you create a three-node cluster that contains Active, Passive, and Witness nodes. Different configuration paths are available. What you select depends on your existing configuration.

Plan the vCenter HA Deployment

Before you can configure vCenter HA, you have to consider several factors. A deployment with components that use different versions of vSphere requires different considerations than a deployment that includes only vSphere 7.0 components. Resource and software requirements and the networking setup must also be considered carefully.

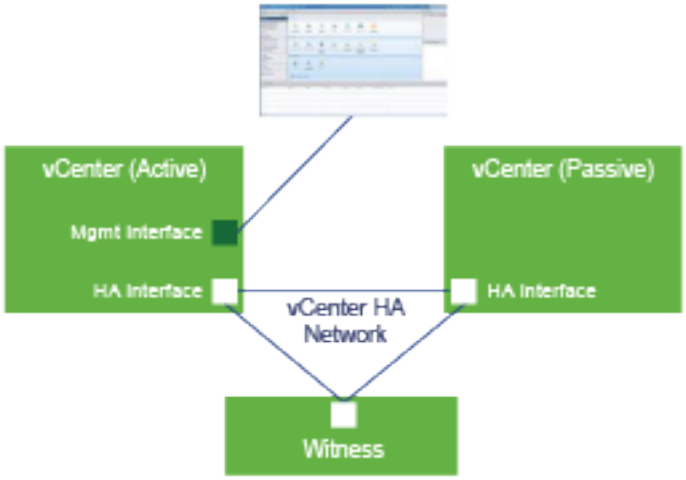
vCenter Architecture Overview

A vCenter HA cluster consists of three vCenter Server instances. The first instance, initially used as the Active node, is cloned twice to a Passive node and to a Witness node. Together, the three nodes provide an active-passive failover solution.

Deploying each of the nodes on a different ESXi instance protects against hardware failure. Adding the three ESXi hosts to a DRS cluster can further protect your environment.

When vCenter HA configuration is complete, only the Active node has an active management interface (public IP). The three nodes communicate over a private network called vCenter HA network that is set up as part of configuration. The Active node is continuously replicating data to the Passive node.

Figure 111: vCenter Three-Node Cluster



All three nodes are necessary for the functioning of this feature. Compare the node responsibilities.

Table 349: vCenter HA Nodes

Node	Description
Active	• Runs the active vCenter Server instance • Uses a public IP address for the management interface • Uses the vCenter HA network for replication of data to the Passive node. • Uses the vCenter HA network to communicate with the Witness node.
Passive	• Is initially a clone of the Active node • Constantly receives updates from and synchronizes state with the Active node over the vCenter HA network • Automatically takes over the role of the Active node if a failure occurs
Witness	• Is a lightweight clone of the Active node • Provides a quorum to protect against a split-brain situations

vCenter HA Hardware and Software Requirements

Before you set up vCenter HA, ensure that you have sufficient memory, CPU, and datastore resources, and ensure that you are using versions of vCenter Server and ESXi that support vCenter HA.

Your environment must meet the following requirements.

Table 350: vCenter HA Requirements

Component	Requirements
ESXi	• ESXi 6.0 or later is required. • A minimum of three ESXi hosts is strongly recommended. Each vCenter HA node can then run on a different host for better protection.
Management vCenter Server (if used)	Your environment can include a management vCenter Server system, or you can set up your vCenter Server to manage the ESXi host on which it runs (self-managed vCenter Server) • vCenter Server 6.0 or later is required.

Component	Requirements
vCenter Server	• vCenter Server 6.5 or later is required. • Deployment size Small (4 CPU and 16GB RAM) or bigger is required to meet the RTO. Do not use Tiny in production environments. • vCenter HA is supported and tested with VMFS, NFS, and vSAN datastores. • Ensure you have enough disk space to collect and store support bundles for all three nodes on the Active node. See Collecting Support Bundles for a vCenter HA Node.
Network connectivity	• vCenter HA network latency between Active, Passive, and Witness nodes must be less than 10 ms. • The vCenter HA network must be on a different subnet than the management network.
Licensing required for vCenter HA	• vCenter HA requires a single vCenter Server license. • vCenter HA requires a Standard license.

vCenter HA Configuration Workflow

To configure the passive and witness nodes in your vCenter HA environment, you can use the **Set Up vCenter HA** wizard. With the manual option, you must manually clone the active node and create the passive and witness nodes.

Note: For automatic and manual configurations, verify that your environment is satisfying the hardware and software requirements. See vCenter HA Hardware and Software Requirements.

Automatic Configuration

You can use the **Set Up vCenter HA** wizard to automatically create the passive and witness nodes as part of vCenter HA configuration.

1. You deploy the first vCenter Server, which will become the active node.
2. You add a second network (port group) for vCenter HA traffic on each ESXi host.
3. You start the vCenter HA configuration and supplies the IP addresses, the target ESXi host or cluster, and the datastore for each clone.
4. The system clones the active node and creates a passive node with precisely the same settings, including the same host name.
5. The system clones the active node again and creates a more light-weight witness node.
6. The system sets up the vCenter HA network on which the three nodes communicate, for example, by exchanging heartbeats and other information.

Manual Configuration

If you want more control over your deployment, you can perform a manual vCenter HA configuration, where you clone the active node and create the passive and witness nodes of your configuration. If you select this option and remove the vCenter HA configuration later, you are responsible for deleting the nodes that you created.

1. You deploy the first vCenter Server, which becomes the active node.
2. You add a second network (port group) for vCenter HA traffic on each ESXi host.
3. You must add a second network adapter (NIC) to the active node if the credentials of the active management vCenter Server are unknown.
4. You log in to the vCenter Server (active node) with the vSphere Client.
5. You start the vCenter HA configuration, select the checkbox to manually configure and supply IP address and subnet information for the passive and witness nodes. Optionally, you can override the failover management IP addresses.
6. After the vCenter HA deployment task finishes, you log in to the management vCenter Server and create two clones of the vCenter Server (active node).

7. The system sets up the vCenter HA network on which the three nodes exchange heartbeats and replication information.
8. The vCenter Server is protected by vCenter HA.

For more information, see Configure vCenter HA With the vSphere Client.

Configure the Network

Regardless of the deployment option and inventory hierarchy that you select, you have to set up your network before you can start configuration. To set the foundation for the vCenter HA network, you add a port group to each ESXi host.

- The vCenter Server that later becomes the Active node, is deployed.
- You can access and have privileges to modify that vCenter Server and the ESXi host on which it runs.
- During network setup, you need static IP addresses for the management network. The management and cluster network addresses must be IPv4 or IPv6. They cannot be mixed mode IP addresses.

After configuration is complete, the vCenter HA cluster has two networks, the management network on the first virtual NIC and the vCenter HA network on the second virtual NIC.

Management network	The management network serves client requests (public IP). The management network IP addresses must be static.
vCenter HA network	The vCenter HA network connects the Active, Passive, and Witness nodes and replicates the server state. It also monitors heartbeats. • The vCenter HA network IP addresses for the Active, Passive, and Witness nodes must be static. • The vCenter HA network must be on a different subnet than the management network. The three nodes can be on the same subnet or on different subnets. • Network latency between the Active, Passive, and Witness nodes must be less than 10 milliseconds. • You must not add a default gateway entry for the cluster network. **Note:** vCenter HA setup is not supported when using a Wide Area Network (WAN) for the networking configuration. VCHA requires a dedicated, high-fidelity, and low-latency network. For more information, see kB 80551.

1. Log in to the management vCenter Server and find the ESXi host on which the Active node is running.
2. Add a port group to the ESXi host.

   This port group can be on an existing virtual switch or, for improved network isolation, you can create a new virtual switch. It must be different from the management network.
3. If your environment includes the recommended three ESXi hosts, add the port group to each of the hosts.

Configure vCenter HA With the vSphere Client

When you use the vSphere Client, the **Set Up vCenter HA** wizard creates and configures a second network adapter on the vCenter Server, clones the Active node, and configures the vCenter HA network.

- Deploy vCenter Server that you want to use as the initial Active node.
  - The vCenter Server must have a static IP address.
  - SSH must be activated on the vCenter Server.

- Verify that your environment meets the following requirements.
  - The vCenter Server that will become the Active node is managing its own ESXi host and its own virtual machine. This configuration is sometimes called a self-managed vCenter Server.
- Set up the infrastructure for the vCenter HA network. See Configure the Network.
- Determine which static IP addresses to use for the two vCenter Server nodes that will become the Passive node and Witness node.

Note: In order to use an NSX-T segment on the Active node, you must create NIC2/eth1 by using **Edit VM Settings** to add the second NIC with the NSX-T segment. You do not need to specify any resources for Passive or Witness nodes, because the Clone must be created using **Clone VM** after adding necessary Guest customization specifications for Passive and Witness containing NIC1/eth0 and NIC2/eth1 with IP addresses. When you configure VCHA IP addresses for eth1 in vCenter Server, the eth1 on the Active Node is automatically filled in.

1. Log in to the Active node with the vSphere Client.
2. Select the vCenter Server object in the inventory and select the **Configure** tab.
3. Select **vCenter HA** under settings.
4. Click on the **Set Up vCenter HA** button to start the setup wizard.
   - If the vCenter server is self-managed, the **Resource settings** page is displayed. Proceed to step 7.
   - If your vCenter server is managed by another vCenter server in the same SSO domain, proceed to step 7.
   - If your vCenter server is managed by another vCenter server in a different SSO domain, input the location and credential details of that management vCenter server.
5. Click **Management vCenter Server credentials**. Specify the Management vCenter server FQDN or IP address, Single Sign-On user name and password and click **Next**.

   If you do not have the Single Sign-On administrator credentials, select the second bullet and click **Next**.
6. You may see a **Certificate warning** displayed. Review the SHA1 thumbprint and select **Yes** to continue.
7. In the **Resource settings** section, first select the vCenter HA network for the active node from the drop-down menu.

   Note: The network selector is no longer visible once NIC2/eth1 is created.
8. Click on the checkbox if you want to automatically create clones for Passive and Witness nodes.

   Note: If you do not select the checkbox, you must manually create clones for Passive and Witness nodes after you click **Finish**.

9. For the Passive node, click **Edit**.
   a) Specify a unique name and target location.
   b) Select the destination compute resource for the operation.
   c) Select the datastore in which to store the configuration and disk files.
   d) Select virtual machine Management (NIC 0) and vCenter HA (NIC 1) networks.
      If there are issues with your selections, errors or compatibility warnings are displayed.
   e) Review your selections and click **Finish**.
10. For the Witness node, click **Edit**.
    a) Specify a unique name and target location.
    b) Select the destination compute resource for the operation.
    c) Select the datastore in which to store the configuration and disk files.
    d) Select vCenter HA (NIC 1) network.
       If there are issues with your selections, errors or compatibility warnings are displayed.
    e) Review your selections and click **Finish**.
11. Click **Next**.
12. In the **IP settings** section, select the IP version from the drop-down menu.
13. Enter the IPv4 address (NIC 1) and Subnet mask or prefix length information for the Active, Passive and Witness nodes.
    You can Edit management network settings for the Passive Node. Customizing these settings are optional. By default, the management network settings of the Active node are applied.
14. Click **Finish**.

The Passive and Witness nodes are created. When **Set Up vCenter HA** is complete, vCenter Server has high availability protection. After vCenter HA is activated, you can click **Edit** to enter Maintenance Mode, Enable or Disable vCenter HA. There are separate buttons to remove vCenter HA or initiate vCenter HA failover.

See Manage the vCenter HA Configuration for a list of cluster management tasks.

For a brief overview of enhancements in the vSphere Client when working with vCenter HA, see:

Manage the vCenter HA Configuration

After you configure your vCenter HA cluster, you can perform management tasks. These tasks include certificate replacement, replacement of SSH keys, and SNMP setup. You can also edit the cluster configuration to deactivate or activate vCenter HA, enter maintenance mode, and remove the cluster configuration.

Set Up SNMP Traps

You can set up Simple Network Management Protocol (SNMP) traps to receive SNMP notifications for your vCenter HA cluster.

The traps default to SNMP version 1.

Set up SNMP traps for the Active node and the Passive node. You tell the agent where to send related traps, by adding a target entry to the snmpd configuration.

1. Log in to the Active node by using the Virtual Machine Console or SSH.
2. Run the `vicfg-snmp` command, for example:

   ```
   vicfg-snmp -t 10.160.1.1@1166/public
   ```

   In this example, `10.160.1.1` is the client listening address, `1166` is the client listening port, and `public` is the community string.
3. Activate the SNMP agent (snmpd) by running the following command.

   ```
   vicfg-snmp -e
   ```

You also might find these commands useful.

- To view the complete help for the command, run `vicfg-snmp -h`.
- To deactivate the SNMP agent, run `vicfg-snmp -D`.
- To show the SNMP agent's configuration, run `vicfg-snmp -s`.
- To reset the configuration to the default, run `vicfg-snmp -r`.

Set Up Your Environment to Use Custom Certificates

The machine SSL certificate on each node is used for cluster management communication and for encryption of replication traffic. If you want to use custom certificates, you have to remove the vCenter HA configuration, delete the Passive and Witness nodes, provision the Active node with the custom certificate, and reconfigure the cluster.

If possible, replace certificates in the vCenter Server that will become the Active node before you clone the node.

1. Edit the cluster configuration and select **Remove**.
2. Delete the Passive node and the Witness node.
3. On the Active node, which is now a standalone vCenter Server, replace the machine SSL Certificate with a custom certificate.
4. Reconfigure the cluster.

Manage vCenter HA SSH Keys

vCenter HA uses SSH keys for password-less authentication between the Active, Passive, and Witness nodes. The authentication is used for heartbeat exchange and file and data replication. To replace the SSH keys in the nodes of a vCenter HA cluster, you deactivate the cluster, generate new SSH keys on the Active node, transfer the keys to the passive node, and activate the cluster.

1. Edit the cluster and change the mode to **Disabled**.
2. Log in to the Active node by using the Virtual Machine Console or SSH.
3. Activate the bash shell.

   ```
   bash
   ```
4. Optionally, back up the contents of the `/home/vcha/.ssh` folder to the Active node.
5. To stop VCHA service on the Active node, run the following command.

   ```
   vmon-cli --stop vcha
   ```
6. To generate new SSH keys on the Active node, run the following command.

   ```
   /usr/sbin/vcha-reset-ssh-keys
   ```

7. Copy the SSH keys to the Passive node and Witness node.

   ```
   scp /home/vcha/.ssh/*
   ```

8. To start the VCHA service on the Active node, run the following command.

   ```
   vmon-cli --start vcha
   ```

9. Edit the cluster configuration and set the vCenter HA cluster to **Enabled**.

The VCHA state changes to **Healthy**.

Initiate a vCenter HA Failover

You can manually initiate a failover and have the Passive node become the Active node.

A vCenter HA cluster supports two types of failover.

Automatic failover	The Passive node attempts to take over the active role in case of an Active node failure.
Manual failover	The user can force a Passive node to take over the active role by using the Initiate Failover action.

Initiate a manual failover for troubleshooting and testing.

1. Log in to the Active node vCenter Server with the vSphere Client and click **Configure** for the vCenter Server where you need to initiate failover.
2. Under **Settings** select **vCenter HA** and click **Initiate Failover**.
3. Click **Yes** to start the failover.

   A dialog offers you the option to force a failover without synchronization. In most cases, performing synchronization first is best.
4. After the failover, you can verify that the Passive node has the role of the Active node in the vSphere Client.

Edit the vCenter HA Cluster Configuration

When you edit the vCenter HA cluster configuration, you can deactivate or activate the cluster, place the cluster in maintenance mode, or remove the cluster.

Verify that the vCenter HA cluster is deployed and contains the Active, Passive, and Witness nodes.

The operating mode of a vCenter Server controls the failover capabilities and state replication in a vCenter HA cluster.

A vCenter HA cluster can operate in one of the following modes.

Table 351: vCenter HA Cluster Modes of Operation

Mode	Automatic Failover	Manual Failover	Replication	
Enabled	Yes	Yes	Yes	This default mode of operation protects the vCenter Server from hardware and software failures by performing automatic failover.
Maintenance	No	Yes	Yes	Used for some maintenance tasks. For other tasks, you have to deactivate vCenter HA.

Mode	Automatic Failover	Manual Failover	Replication	
Disabled	No	No	No	If the Passive or Witness nodes are lost or recovering from a failure, a vCenter HA configuration can be deactivated. The Active node continues as a standalone vCenter Server.

Note: If the cluster is operating in either Maintenance or Disabled mode, an Active node can continue serving client requests even if the Passive and Witness nodes are lost or unreachable.

1. Log in to the Active node vCenter Server with the vSphere Client and click **Configure**.
2. Under **Settings** select **vCenter HA** and click **Edit**.
3. Select one of the options.

Option	Result
Enable vCenter HA	Activates replication between the Active and Passive nodes. If the cluster is in a healthy state, your Active node is protected by automatic failover from the Passive node.
Maintenance Mode	In maintenance mode, replication still occurs between the Active and Passive nodes. However, automatic failover is deactivated.
Disable vCenter HA	Deactivates replication and failover. Keeps the configuration of the cluster. You can later activate vCenter HA again.
Remove vCenter HA cluster	Removes the cluster. Replication and failover no longer are provided. The Active node continues to operate as a standalone vCenter Server. See Remove a vCenter HA Configuration for details.

4. Click OK.

Perform Backup and Restore Operations

For additional security, you can back up the Active node in the vCenter HA cluster. You can then restore the node in case of catastrophic failure.

Verify the interoperability of vCenter HA and the backup and restore solution. One solution is vCenter Server file-based restore.

Note: Remove the cluster configuration before you restore the Active node. Results are unpredictable if you restore the Active node and the Passive node is still running or other cluster configuration is still in place.

1. Back up the Active node.

   Do not back up the Passive node and Witness node.
2. Before you restore the cluster, power off and delete all vCenter HA nodes.
3. Restore the Active node.

   The Active node is restored as a standalone vCenter Server.

4. Reconfigure the vCenter HA.

Remove a vCenter HA Configuration

You can remove a vCenter HA configuration from the vSphere Client.

1. Log in to the Active node vCenter Server and click **Configure**.
2. Under **Settings** select **vCenter HA** and click **Remove VCHA**.
   - The vCenter HA cluster's configuration is removed from the Active, Passive, and Witness nodes.
   - You can choose to delete the Passive and Witness nodes.
   - The Active node continues to run as a standalone vCenter Server.
   - You cannot reuse the Passive and Witness nodes in a new vCenter HA configuration.
   - If you performed a manual configuration, or if the Passive and Witness nodes are not discoverable, you must delete these nodes explicitly.
   - Even if the second virtual NIC was added by the configuration process, the removal process does not remove the virtual NIC.

Reboot All vCenter HA Nodes

If you have to shut down and reboot all nodes in the cluster, you must follow a specific shutdown order to prevent the Passive node from assuming the role of Active node.

1. Shut down the nodes in this order.
   - Passive node
   - Active node
   - Witness node
2. Restart each node.

   You can restart nodes in any order.
3. Verify that all nodes join the cluster successfully, and that the previous Active node resumes that role.

Change the Server Environment

When you deploy a vCenter Server, you select an environment. For vCenter HA, Small, Medium, Large, and X-Large are supported for production environments. If you need more space and want to change the environment, you have to delete the Passive node virtual machine before you change the configuration.

1. Log in to the Active node with the vSphere Client, edit the cluster configuration, and select **Disable**.
2. Delete the Passive node virtual machine.
3. Change the vCenter Server configuration for the Active node, for example, from a Small environment to a Medium environment.
4. Reconfigure vCenter HA.

Collecting Support Bundles for a vCenter HA Node

Collecting a support bundle from all the nodes in a vCenter HA cluster helps with troubleshooting.

When you collect a support bundle from the Active node in a vCenter HA cluster, the system proceeds as follows.

- Collects support bundle information from the Active node itself.

- Collects support bundles from Passive and Witness nodes and places them in the `commands` directory on the Active node support bundle.

Note: The collection of support bundles from the Passive and Witness nodes is a best effort and happens if the nodes are reachable.

Troubleshoot Your vCenter HA Environment

In case of problems you can troubleshoot your environment. The task you need to perform depends on the failure symptoms. For additional troubleshooting information, see the VMware Knowledge Base system.

vCenter HA Clone Operation Fails During Deployment

If the vCenter HA configuration process does not create the clones successfully, you have to resolve that cloning error.

Clone operation fails.

Note: Cloning a Passive or Witness VM for a VCHA deployment to the same NFS 3.1 datastore as the source Active node VM fails. You must use NFS4 or clone the Passive and Witness VMs to a datastore different from the Active VM.

Look for the clone exception. It might indicate one of the following problems.

- You have a DRS-enabled cluster, but do not have three hosts.
- The host or database connection is lost.
- Not enough disk space.
- Other **Clone Virtual Machine** errors

1. Resolve the error that caused the problem.
2. Remove the cluster and start configuration again.

Redeploy the Passive or Witness node

If the passive or witness node fails and vCenter HA cluster was configured using the automatic cloning method, you can redeploy it in the **vCenter HA Settings** page.

1. Log in to the Active node with the vSphere Client.
2. Select the vCenter Server object in the inventory and select the **Configure** tab.
3. Select **vCenter HA** under **Settings**.
4. Click on the **REDEPLOY** button next to the node to start the Redeploy wizard.
5.
   - If your vCenter server is managed by another vCenter server in the same SSO domain, proceed to step 6.
   - If your vCenter server is managed by another vCenter server in a different SSO domain, input the location and credential details of that management vCenter server. Enter the **Management vCenter Server FQDN or IP address** and **Single Sign-On** credentials.

6. Specify a unique name and target location.
7. Select the destination compute resource for the operation.
8. Select the datastore in which to store the configuration and disk files.
9. Configure the virtual machine networks.
   - If you are redeploying the Passive node, select virtual machine Management (NIC 0) and vCenter HA (NIC 1) networks.
   - If you are redeploying the Witness node, select vCenter HA (NIC 1) network.

   If there are issues with your selections, errors or compatibility warnings are displayed.
10. Review your selections and click **Finish** to redeploy the node.

vCenter HA Deployment Fails with an Error

Deployment failures can be caused by configuration issues, especially problems with the networking setup.

You start a vCenter HA cluster configuration, and it fails with an error. The error might show the cause of the problem, for example, you might see an SSH Connection Failed message.

If deployment fails, take steps to resolve the network issues.

1. Verify that the Passive and Witness nodes can be reached from the Active node.
2. Verify that routing between the nodes is set up correctly.
3. Check network latency.

Troubleshooting a Degraded vCenter HA Cluster

For a vCenter HA cluster to be healthy, each of the Active, Passive, and Witness nodes must be fully operational and be reachable over the vCenter HA cluster network. If any of the nodes fails, the cluster is considered to be in a degraded state.

If the cluster is in a degraded state, failover cannot occur. For information about failure scenarios while the cluster is in a degraded state, see Failover Failures.

The cluster can be in a degraded state for a number of reasons.

One of the nodes fails	• If the Active node fails, a failover of the Active node to the Passive node occurs automatically. After the failover, the Passive node becomes the Active node. At this point, the cluster is in a degraded state because the original Active node is unavailable. After the failed node is repaired or comes online, it becomes the new Passive node and the cluster returns to a healthy state after the Active and Passive nodes synchronize. • If the Passive node fails, the Active node continues to function, but no failover is possible and the cluster is in a degraded state. If the Passive node is repaired or comes online, it automatically rejoins the cluster and the cluster state is healthy after the Active and Passive nodes synchronize. • If the Witness node fails, the Active node continues to function and replication between Active and Passive node continues, but no failover can occur. If the Witness node is repaired or comes online, it automatically rejoins the cluster and the cluster state is healthy.

Database replication fails	If replication fails between the Active and Passive nodes, the cluster is considered degraded. The Active node continues to synchronize with the Passive node. If it succeeds, the cluster returns to a healthy state. This state can result from network bandwidth problems or other resource shortages.
Configuration file replication issues	If configuration files are not properly replicated between the Active and Passive nodes, the cluster is in a degraded state. The Active node continues to attempt synchronization with the Passive node. This state can result from network bandwidth problems or other resource shortages.

How you recover depends on the cause of the degraded cluster state. If the cluster is in a degraded state, events, alarms, and SNMP traps show errors.

If one of the nodes is down, check for hardware failure or network isolation. Check whether the failed node is powered on.

In case of replication failures, check if the vCenter HA network has sufficient bandwidth and ensure network latency is 10 ms or less.

Recovering from Isolated vCenter HA Nodes

If all nodes in a vCenter HA cluster cannot communicate with each other, the Active node stops serving client requests.

Node isolation is a network connectivity problem.

1. Attempt to resolve the connectivity problem. If you can restore connectivity, isolated nodes rejoin the cluster automatically and the Active node starts serving client requests.
2. If you cannot resolve the connectivity problem, you have to log in to Active node's console directly.
   a) Power off and delete the Passive node and the Witness node virtual machines.
   b) Log in to the Active node by using SSH or through the Virtual Machine Console.
   c) To enable the Bash shell, enter `shell` at the `appliancesh` prompt.
   d) Run the following command to remove the vCenter HA configuration.

      ```
      vcha-destroy -f
      ```

   e) Reboot the Active node.

      The Active node is now a standalone vCenter Server.
   f) Perform vCenter HA cluster configuration again.

Resolving Failover Failures

When a Passive node does not become the Active node during a failover, you can force the Passive node to become the Active node.

The Passive node fails while trying to assume the role of the Active node.

A vCenter HA failover might not succeed for these reasons.

- The Witness node becomes unavailable while the Passive node is trying to assume the role of the Active node.
- An server state synchronization issue between the nodes exists.

You recover from this issue as follows.

1. If the Active node recovers from the failure, it becomes the Active node again.

2. If the Witness node recovers from the failure, follow these steps.
   a. Log in to the Passive node through the Virtual Machine Console.
   b. To enable the Bash shell, enter `shell` at the `appliancesh` prompt.
   c. Run the following command.
      ```
      vcha-reset-primary
      ```
   d. Reboot the Passive node.
3. If both Active node and Witness node cannot recover, you can force the Passive node to become a standalone vCenter Server.
   a. Delete the Active node and Witness node virtual machines.
   b. Log in to the Passive node through the Virtual Machine Console.
   c. To enable the Bash shell, enter `shell` at the `appliancesh` prompt.
   d. Run the following command.
      ```
      vcha-destroy
      ```
   e. Reboot the Passive node.

VMware vCenter® HA Alarms and Events

If a vCenter HA cluster is in a degraded state, alarms and events show errors.

Table 352: The following events will raise VCHA health alarm in vpxd:

Event Name	Event Description	Event Type	Category
vCenter HA cluster state is currently healthy	vCenter HA cluster state is currently healthy	com.vmware.vcha.cluster.state.healthy	info
vCenter HA cluster state is currently degraded	vCenter HA cluster state is currently degraded	com.vmware.vcha.cluster.state.degraded	warning
vCenter HA cluster state is currently isolated	vCenter HA cluster state is currently isolated	com.vmware.vcha.cluster.state.isolated	error
vCenter HA cluster is destroyed	vCenter HA cluster is destroyed	com.vmware.vcha.cluster.state.destroyed	info

Table 353: The following events will raise PSC HA health alarm in vpxd:

Event Name	Event Description	Event Type	Category
PSC HA state is currently healthy	PSC HA state is currently healthy	com.vmware.vcha.psc.ha.health.healthy	info
PSC HA state is currently degraded	PSC HA state is currently degraded	com.vmware.vcha.psc.ha.health.degraded	info
PSC HA is not monitored after vCenter HA cluster is destroyed	PSC HA state is not being monitored	com.vmware.vcha.psc.ha.health.unknown	info

Table 354: Cluster Status Related Events

Event Name	Event Description	Event Type	Category
Node {nodeName} joined back to the cluster	One node joined back to the cluster	com.vmware.vcha.node.joined	info

Event Name	Event Description	Event Type	Category
Node {nodeName} left the cluster	One node left the cluster	com.vmware.vcha.node.left	warning
Failover succeeded	Failover succeeded	com.vmware.vcha.failover.succeeded	info
Failover cannot proceed when cluster is in disabled mode	Failover cannot proceed when cluster is in disabled mode	com.vmware.vcha.failover.failed.disabledmode	warning
Failover cannot proceed when cluster does not have all three nodes connected	Failover cannot proceed when cluster does not have all three nodes connected	com.vmware.vcha.failover.failed.nodedown	warning
Failover cannot proceed when vPostgres on Passive node is not ready to takeover	Failover cannot proceed when Passive node is not ready to takeover	com.vmware.vcha.failover.failed.passivenotready	warning
vCenter HA cluster mode changed to {clusterMode}	vCenter HA cluster mode changed	com.vmware.vcha.cluster.mode.changed	info

Table 355: Database replication-related events

Event Name	Event Description	Event Type	Category
Database replication mode changed to {newState}	Database replication state changed: sync, async or no replication	com.vmware.vcha.DB.replication.state.changed	info

Table 356: File replication-related events

Event Name	Event Description	Event Type	Category
Appliance {fileProviderType} is {state}	Appliance File replication state changed	com.vmware.vcha.file.replication.state.changed	info

Patching a vCenter High Availability Environment

You can patch a vCenter Server which is in a vCenter High Availability cluster by using the `software-packages` utility available in the vCenter Server shell.

For more information, see *Patch a vCenter High Availability Environment* in *vSphere Upgrade*.

vSphere Monitoring and Performance

VMware provides several tools to help you monitor your virtual environment and to locate the source of potential issues and current problems.

Performance Charts	Allow you to see performance data on a variety of system resources including CPU, Memory, Storage, and so on.
Performance Monitoring Command-line Utilities	Allow you to access detailed information on system performance through the command line.
Host Health	Allows you to quickly identify which hosts are healthy and which are experiencing problems.
Events, Alerts, and Alarms	Allow you to configure alerts and alarms and to specify the actions the system should take when they are triggered.
System Log Files	System logs contain additional information about activities in your vSphere environment.

Intended Audience

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

The content in this section is intended for vSphere administrators who perform the following tasks:

- Monitor the health and performance of physical hardware backings for the virtual environment.
- Monitor the health and performance of virtual devices in the virtual environment.
- Troubleshoot problems in the system.
- Configure alarms.
- Configure SNMP messages.
- Use vCenter Events for forensic analysis and auditing of the user actions in the virtual environment.

Virtual machine administrators also might find the section on Monitoring Guest Operating System Performance helpful.

Updated Information

This *vSphere Monitoring and Performance* guide is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Monitoring and Performance* guide.

Revision	Description
09 APR 2024	• Updated the URL in Configure Syslog on ESXi Hosts. • Updated the information about running scrips in Specify Alarm Rules.
05 OCT 2021	Initial release.

Monitoring Inventory Objects with Performance Charts

The vSphere statistics subsystem collects data on the resource usage of inventory objects. Data on a wide range of metrics is collected at frequent intervals, processed, and archived in the vCenter Server database. You can access statistical information through command-line monitoring utilities or by viewing performance charts in the vSphere Client.

Counters and Metric Groups

vCenter Server systems and hosts use data counters to query for statistics. A data counter is a unit of information relevant to a given inventory object or device. Each counter collects data for a different statistic in a metric group. For example, the disk metric group includes separate data counters to collect data for disk read rate, disk write rate, and disk usage. Statistics for each counter are rolled up after a specified collection interval. Each data counter consists of several attributes that are used to determine the statistical value collected.

For a complete list and description of performance metrics, see the *vSphere API Reference*.

Note: Counters that are introduced in later versions might not contain data from hosts of earlier versions. For details, see the VMware Knowledge Base.

Collection Levels and Collection Intervals

Collection levels determine the number of counters for which data is gathered during each collection interval. Collection intervals determine the time period during which statistics are aggregated, calculated, rolled up, and archived in the vCenter Server database. Together, the collection interval and collection level determine how much statistical data is collected and stored in your vCenter Server database.

Data Availability

Real-time data appears in the performance charts only for hosts and virtual machines that are powered on. Historical data appears for all supported inventory objects, but might be unavailable during certain circumstances.

Performance Chart Types

Performance metrics are displayed in different types of charts, depending on the metric type and object.

Table 357: Performance Chart Types

Chart Type	Description
Line chart	Displays metrics for a single inventory object. The data for each performance counter is plotted on a separate line in the chart. For example, a network chart for a host can contain two lines: one showing the number of packets received, and one showing the number of packets transmitted.
Bar chart	Displays storage metrics for datastores in a selected data center. Each datastore is represented as a bar in the chart. Each bar displays metrics based on the file type: virtual disks, snapshots, swap files, and other files.
Pie chart	Displays storage metrics for a single object, based on the file types, or virtual machines. For example, a pie chart for a datastore can display the amount of storage space occupied by the virtual machines taking up the largest space.
Stacked chart	Displays metrics for the child objects that have the highest statistical values. All other objects are aggregated, and the sum value is displayed with the term **Other**. For example, a host's stacked CPU usage chart displays CPU usage metrics for the 10 virtual machines on the host that are consuming the most CPU. The **Other** amount contains the total CPU usage of the remaining virtual machines. The metrics for the host itself are displayed in separate line charts. Stacked charts are useful in comparing the resource allocation and usage across multiple hosts or virtual machines. By default, the 10 child objects with the highest data counter values are displayed.

Data Counters

Each data counter includes several attributes that are used to determine the statistical value collected. See the *vSphere API Reference* for a complete list and description of supported counters.

Table 358: Data Counter Attributes

Attribute	Description
Unit of Measurement	Standard in which the statistic quantity is measured. • Kilobytes (KB) – 1024 bytes **Note:** Technically, 1 Kilobytes (KB) = 1000 bytes and 1 Kibibyte (KiB) = 1024 bytes. However, based on the context, kilobyte is also used for 1024 bytes in the computer science literature interchangeably. • Kilobytes per second (KBps) – 1024 bytes per second • Kilobits (kb) – 1000 bits • Kilobits per second (kbps) – 1000 bits per second • Megabytes (MB) • Megabytes per second (MBps) • Megabits (Mb), megabits per second (Mbps) • Megahertz (MHz) • Microseconds (µs) • Milliseconds (ms) • Number (#) • Percent (%) • Seconds (s) • Watts (watt) • Joules (joule) • Terabytes (teraBytes) • Temperature in celsius (celsius)
Description	Text description of the data counter.
Statistics Type	Measurement used during the statistics interval. Related to the unit of measurement. • Rate – Value over the current statistics interval. For example: CPU Usage: Amount of CPU actively used by the host, resource pool, or virtual machine in the cluster. Counter: usagemhz Stats Type: Rate Unit: MegaHertz (MHz) • Delta – Change from previous statistics interval. For example: CPU System Time for vCPU (%): Amount of time spent on system processes on each virtual CPU in the virtual machine. **Note:** This is the host view of the CPU usage, not the guest operating system view. Counter: system Stats Type: Delta Unit: Percentage (%) • Absolute – Absolute value (independent of the statistics interval). For example: Memory: Amount of host machine memory used by all powered on virtual machines in the cluster. A cluster's consumed memory consists of virtual machine consumed memory and overhead memory. It does not include host-specific overhead memory, such as memory used by the service console or VMkernel. Counter: consumed Stats Type: Absolute Unit: MegaBytes (MB)
Rollup Type	Calculation method used during the statistics interval to aggregate data. Determines the type of statistical values that are returned for the counter.

Attribute	Description
	• Average – Data collected during the interval is aggregated and averaged. For example: Virtual Disk Read Requests: Number of virtual disk read commands completed on each virtual disk on the virtual machine. The aggregate number of all virtual disk read commands is also displayed in the chart. Counter: numberRead Stats Type: Absolute Unit: Number Rollup Type: Average • Minimum – The minimum value is rolled up. • Maximum – The maximum value is rolled up. The Minimum and Maximum values are collected and displayed only in statistics level 4. Minimum and maximum rollup types are used to capture peaks in data during the interval. For real-time data, the value is the current minimum or current maximum. For historical data, the value is the maximum or minimum of the aggregated values. For example, the following information for the CPU usage chart shows that the average is collected at statistics level 1. The minimum and maximum values are collected at statistics level 4. – Counter: usage – Unit: Percentage (%) – Rollup Type: Average (Minimum/Maximum) – Collection Level: 1 (4) • Summation – Data collected is summed. The measurement displayed in the chart represents the sum of data collected during the interval. For example: Network Packets Received: Number of network packets received across the top ten physical NIC instances on the host. The chart also displays the aggregated value for all NICs. Counter: packetRx Stats Type: Absolute Unit: Number Rollup Type: Summation • Latest – Data collected during the interval is a set value. The value displayed in the performance charts represents the current value. For example: Space in GB (Allocated): Total amount of logical datastore space provisioned by an administrator for the virtual machine. It is the storage size up to which the virtual machine files on datastores can grow. This includes log files, VMX files, and other miscellaneous files. Allocated space is not always in use. Counter: provisioned Stats Type: Absolute Unit: Gigabytes (GB) Rollup Type: Latest
Collection level	A collection level determines the number of data counters used to collect statistics data. Collection levels are also referred as statistics levels. These collection levels vary from 1 to 4, with Level 4 having the most counters. • Level 1 is the least detailed statistics level and only includes the most critical statistics, such as aggregate CPU, memory, and network usage. • Level 2 introduces a number of additional statistics • Level 3 incorporates per instance statistics, for example CPU usage of a host on a per-CPU basis. • Level 4 is the most detailed and is inclusive of all the other levels For more information on collection levels, see Data Collection Levels . **Note:** Be careful when you set a higher collection level, as the process requires significant increase of resource usage.

Metric Groups in vSphere

The performance data collection subsystem for vSphere collects performance data on various inventory items and their devices. Data counters define individual performance metrics. Performance metrics are organized into logical groups based on the object or object device. Statistics for one or more metrics can be displayed in a chart.

Table 359: Metric Groups

Metric group	Description
Cluster Services	Performance statistics for clusters configured by using vSphere Distributed Resource Scheduler, vSphere High Availability, or both.
CPU	CPU utilization per host, virtual machine, resource pool, or compute resource.
Datastore	Statistics for datastore utilization. **Note:** From VC 4.1 onwards, NFS statistics are collected under datastore statistics.
Disk	Disk utilization per host, virtual machine, or datastore. Disk metrics include I/O performance, such as latency and read/write speeds, and utilization metrics for storage as a finite resource.
Memory	Memory utilization per host, virtual machine, resource pool, or compute resource. The value obtained is one of the following: • For virtual machines, memory refers to the guest physical memory. Guest physical memory is the amount of physical memory presented as a virtual-hardware component to the virtual machine, at creation time, and made available when the virtual machine is running. • For hosts, memory refers to the machine memory. Machine memory is the RAM that is installed on the hardware that comprises the host.
Network	Network utilization for both physical and virtual network interface controllers (NICs) and other network devices. The virtual switches that support connectivity among all components, such as hosts, virtual machines, VMkernel.
Power	Energy usage statistics per host.
Storage Adapter	Data traffic statistics per host bus adapter (HBA).
Storage Path	Data traffic statistics per path.
System	Overall system availability, such as the system heartbeat and uptime. These counters are available directly from hosts and from vCenter Server.
Virtual Disk	Disk utilization and disk performance metrics for virtual machines.
Virtual Flash	Virtual flash counters.
Virtual Machine Operations	Virtual machine power and provisioning operations in a cluster or data center.
vSphere Replication	Statistics for the virtual machine replication performed by VMware vCenter Site Recovery Manager.

Data Collection Intervals

Collection intervals determine the duration for which statistics are aggregated, calculated, rolled up, and archived. Together, the collection interval and collection level determine how much statistical data is gathered and stored in your vCenter Server database.

Table 360: Collection Intervals

Collection Interval/ Archive Length	Collection Frequency	Default Behavior
1 Day	5 Minutes	Real-time (20s) statistics are rolled up to create one data point every 5 minutes. The result is 12 data points every hour and 288 data points every day. After 30 minutes, the six data points collected are aggregated and rolled up as a data point for the 1-Week time range. You can change the interval duration and archive length of the 1-Day collection interval by configuring the statistics settings.
1 Week	30 Minutes	1-Day statistics are rolled up to create one data point every 30 minutes. The result is 48 data points every day and 336 data points every week. Every 2 hours, the 12 data points collected are aggregated and rolled up as a data point for the 1-Month time range. You cannot change the default settings of the 1-Week collection interval.
1 Month	2 Hours	1-Week statistics are rolled up to create one data point every 2 hours. The result is 12 data points every day and 360 data points every month (assuming a 30-day month). After 24 hours, the 12 data points collected are aggregated and rolled up as a data point for the **1-Year** time range. You cannot change the default settings of the 1-Month collection interval.
1 Year	1 Day	1-Month statistics are rolled up to create one data point every day. The result is 365 data points each year. You can change the archive length of the 1-Year collection interval by configuring the statistics settings.

Note: If you change the duration of data collection intervals you might need to allocate more storage resources.

Data Collection Levels

Each collection interval has a default collection level that determines the amount of data gathered and which counters are available for display in the charts. Collection levels are also referred to as statistics levels.

Table 361: Statistics Levels

Level	Metrics	Best Practice
Level 1	• Cluster Services (VMware Distributed Resource Scheduler) – all metrics • CPU – cpuentitlement, totalmhz, usage (average), usagemhz • Disk – capacity, maxTotalLatency, provisioned, unshared, usage (average), used • Memory – consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon), totalbandwidth (DRAM or PMem) • Network – usage (average), IPv6 • System – heartbeat, uptime • Virtual Machine Operations – numChangeDS, numChangeHost, numChangeHostDS	Use for long-term performance monitoring when device statistics are not required. Level 1 is the default Collection Level for all Collection Intervals.
Level 2	• Level 1 metrics • CPU – idle, reservedCapacity • Disk – All metrics, excluding numberRead and numberWrite. • Memory – All metrics, excluding memUsed, maximum and minimum rollup values, read or write latency (DRAM or PMem).	Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.

Level	Metrics	Best Practice
	• Virtual Machine Operations – All metrics	
Level 3	• Level 1 and Level 2 metrics • Metrics for all counters, excluding minimum and maximum rollup values. • Device metrics	Use for short-term performance monitoring after encountering problems or when device statistics are required.
Level 4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	Use for short-term performance monitoring after encountering problems or when device statistics are required.

Note:

When the statistics levels, level 3 or level 4 are used beyond the default value, it may cause one particular process, vpxd, to sustain memory growth, if it cannot save the statistics information to the database as quickly as required. If the usage limit of these statistics levels is not monitored closely, it may cause vpxd to grow out of memory and eventually crash.

So, in case the administrator decides to elevate any of these levels, it is necessary for the administrator to monitor the size of the vpxd process to make sure that is not growing boundlessly after the change.

View Performance Charts

The vCenter Server statistics settings, the type of object selected, and the features that are enabled on the selected object determine the amount of information displayed in charts. Charts are organized into views. You can select a view to see related data together on one screen. You can also specify the time range, or data collection interval. The duration extends from the selected time range to the present time.

Overview charts display multiple data sets in one panel to evaluate different resource statistics, display thumbnail charts for child objects. It also displays charts for a parent and a child object. Advanced charts display more information than overview charts, are configurable, and can be printed or exported. You can export data in the `PNG`, `JPEG`, or `CSV` formats. See View Advanced Performance Charts.

1. Select a valid inventory object in the vSphere Client.

   Overview and advanced performance charts are available for datacenter, cluster, host, resource pool, vApp, and virtual machine objects. Overview charts are also available for datastores and datastore clusters. Performance charts are not available for network objects.

2. Click the **Monitor** tab, and click **Performance**.
3. Select a view.

   Available views depend on the type of object. For views that might contain many charts in a large environment, the vSphere Client displays the charts distributed on multiple pages. You can use the arrow buttons to navigate between pages.

4. Select a predefined or custom time range.

Performance Charts Options Available Under the View Menu

The performance chart options that you can access under the **View** menu vary depending on the type of inventory object you select.

For example, the **Virtual Machines** view is available when you view host performance charts only if there are virtual machines on the selected host. Likewise, the **Fault Tolerance** view for virtual machine performance charts is available only when that feature is enabled for the selected virtual machine.

Table 362: Performance Chart Views by Inventory Object

Object	View List Items
Data center	• **Storage** - space utilization charts for datastores in the data center, including space by file type and storage space used by each datastore in the data center. • **Clusters** - thumbnail CPU and memory charts for each cluster, and stacked charts for total CPU and memory usage in the data center. This view is the default.
Datastore and datastore cluster	• **Space** - space utilization charts for the datastore: — space utilization by file type — space utilization by virtual machine — space usage • **Performance** - performance charts for the datastore or datastore cluster and for virtual machine disks on the resource. **Note:** The Performance view for datastores is only available when all hosts that are connected to the datastores are ESX/ESXi 4.1 or greater. The Performance view for datastore clusters is only available when the Storage DRS is enabled.
Cluster	• **Home** - CPU and memory charts for the cluster. • **Resource Pools & Virtual Machines** - thumbnail charts for resource pools and virtual machines, and stacked charts for total CPU and memory usage in the cluster. • **Hosts** - thumbnail charts for each host in the cluster, and stacked charts for total CPU, memory, disk usage, and network usage.
Host	• **Home** - CPU, memory, disk, and network charts for the host. • **Virtual Machines** - thumbnail charts for virtual machines, and stacked charts for total CPU usage and total memory usage on the host.
Resource Pool and vApps	• **Home** - CPU and memory charts for the resource pool. • **Resource Pools & Virtual Machines** - thumbnail charts for resource pools, and virtual machines and stacked charts for CPU and memory usage in the resource pool or vApp.
Virtual Machine	• **Storage** - space utilization charts for the virtual machine: space by file type, space by datastore, and total gigabytes. • **Fault Tolerance** - CPU and memory charts that display comparative metrics for the fault-tolerant primary and secondary virtual machines. • **Home** - CPU, memory, network, host (thumbnail charts), and disk usage charts for the virtual machine.

Overview Performance Charts

The overview performance charts display the metrics for an object in the inventory. Use these charts to monitor and troubleshoot performance problems.

The metrics provided in Overview performance charts are a subset of those collected for hosts and the vCenter Server. For a complete list of all metrics collected by hosts and the vCenter Server, see the *vSphere API Reference*.

Clusters

The cluster charts contain information about CPU, disk, memory, and network usage for clusters. The help topic for each chart contains information about the data counters displayed in that chart. The collection level set for vCenter Server determines the available counters.

CPU (MHz)

The CPU (MHz) chart displays CPU usage for the cluster.

Cluster Counters

This chart is located in the Home view of the Cluster **Performance** tab.

Table 363: Data Counters

Chart Label	Description
Usage	Sum of the average CPU usage values, in Megahertz, of all virtual machines in the cluster. • Counter: usagemhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Total	Total amount of CPU resources available in the cluster. The maximum value is equal to the number of cores multiplied by the frequency of the processors. For example, a cluster has two hosts, each of which has four CPUs that are 3 GHz each, and one virtual machine that has two virtual CPUs. VM totalmhz = 2 vCPUs * 3000 MHz = 6000 MHz Host totalmhz = 4 CPUs * 3000 MHz = 12000 MHz Cluster totalmhz = 2 x 4 * 3000 MHz = 24000 MHz • Counter: totalmhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Summation • Collection Level: 1

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of cluster resources. However, if the value is constantly high, the CPU demanded is likely greater than the CPU capacity available. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the hosts in the cluster.

If performance is impacted, consider taking the following actions.

Table 364: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
3	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. This might help avoid hot spots in the cluster.
4	Migrate one or more virtual machines to a new host.
5	Upgrade the physical CPUs or cores on each host in the cluster if necessary.

#	Resolution
6	Enable CPU-saving features, such as TCP Segmentation Offload.
7	Replace software I/O with the dedicated hardware, such as iSCSI HBAs or TCP Segmentation Offload NICs.

CPU Usage

The cluster CPU Usage charts monitor the CPU utilization of the hosts, resource pools, and virtual machines in the cluster. This chart displays the 10 child objects in the cluster with the most CPU usage.

This chart is located in the Resource Pools and Virtual Machines view of the Cluster **Performance** tab.

Table 365: Data Counters

Chart Label	Description
<host>, <resource pool>, or <virtual machine>	Amount of CPU actively used by the host, resource pool, or virtual machine in the cluster. • Counter: usagemhz • Stats Type: Rate • Unit: MegaHertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of cluster resources. However, if the value is constantly high, the CPU demanded is likely greater than the CPU capacity available. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the hosts in the cluster.

If performance is impacted, consider taking the following actions.

Table 366: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
3	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. This might help avoid hot spots in the cluster.
4	Migrate one or more virtual machines to a new host.
5	Upgrade the physical CPUs or cores on each host in the cluster if necessary.
6	Enable CPU-saving features, such as TCP Segmentation Offload.
7	Replace software I/O with the dedicated hardware, such as iSCSI HBAs or TCP Segmentation Offload NICs.

Disk (KBps)

The Disk (KBps) chart displays the disk I/O of the 10 hosts in the cluster with the most disk usage.

This chart is located in the Hosts view of the cluster **Performance** tab.

Table 367: Data Counters

Chart Label	Description
host_name	Average data I/O rate across all hosts in the cluster. • Counter: usage • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 368: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.

#	Resolution
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Memory (MB)

The Memory (MB) chart displays consumed memory for the cluster. The chart appears only at collection level 1.

This chart is located in the Home view of the cluster **Performance** tab.

Table 369: Data Counters

Chart Label	Description
Consumed	Amount of host machine memory used by all powered on virtual machines in the cluster. A cluster's consumed memory consists of virtual machine consumed memory and overhead memory. It does not include host-specific overhead memory, such as memory used by the service console or VMkernel. • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Total	Total amount of machine memory of all hosts in the cluster that is available for virtual machine memory (physical memory for use by the Guest OS) and virtual machine overhead memory. Memory Total = Aggregate host machine memory - (VMkernel memory + Service Console memory + other service memory) **Note:** The totalmb data counter is the same as the effectivemem data counter, which is supported only for backward compatibility. • Counter: totalmb • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Memory usage is not necessarily an indicator of performance problems. Memory can be high if a host is swapping or ballooning, which can result in virtual machine guest swapping. In such cases, check for other problems, such as CPU over-commitment or storage latencies.

If you have constantly high memory usage in a cluster, resource pool, or vApp, consider taking the following actions.

Table 370: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	Verify that the balloon driver is enabled. The balloon driver is installed with VMware Tools and is critical to performance. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.
3	If the balloon value is high, check the resource shares, reservations, and limits for the virtual machines and resource pools on the hosts. Verify that the host's settings are adequate and not lower than those set for the virtual machine. If free memory is available on the hosts and the virtual machines are experiencing high swap or balloon memory, the virtual machine (or resource pool, if it belongs to one) has reached its resource limit. Check the maximum resource limit set on that host.
4	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
5	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. It might help avoid hot spots in the cluster.
6	Add more physical memory to one or more hosts.

Memory (MB)

The Memory (MB) chart displays memory data counters for clusters. The chart appears at all collection levels except level 1.

Description

This chart is located in the **Home** view of the cluster **Performance** tab.

Note: These data counter definitions are for hosts. At the cluster level, the values are collected and totaled. The counter values in the chart represent the aggregate amounts of the host data. The counters that appear in the chart depend on the collection level set for your vCenter Server.

Table 371: Data Counters

Chart Label	Description
Active	Sum of the active guest physical memory of all powered on virtual machines on the host, plus memory used by basic VMkernel applications. Active memory is estimated by the VMkernel. • Counter: active • Stats Type: Absolute

Chart Label	Description
	• Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Balloon	Sum of the guest physical memory reclaimed by the balloon driver for all powered on virtual machines on the host. • Counter: vmmemctl • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Consumed	Amount of machine memory used on the host. Consumed memory includes virtual machine memory, service console memory, and VMkernel memory. consumed memory = total host memory - free host memory • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Granted	Sum of the guest physical memory granted for all powered on virtual machines. Granted memory is mapped to the host's machine memory. Granted memory for a host includes the shared memory of each virtual machine on the host. • Counter: granted • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Swap Used	Sum of the memory swapped by all powered on virtual machines on the host. • Counter: swapused • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Total	Aggregate total memory available to the cluster. • Counter: totalmb • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

To ensure best performance, the host memory must be large enough to accommodate the active memory of the virtual machines. The active memory can be smaller than the virtual machine memory size. It allows you to over-provision memory, but still ensures that the virtual machine active memory is smaller than the host memory.

Transient high-usage values usually do not cause performance degradation. For example, memory usage can be high when several virtual machines are started at the same time or when a spike occurs in virtual machine workload. However, a consistently high memory usage value (94% or greater) indicates that the host is probably lacking the memory required to meet the demand. If the active memory size is the same as the granted memory size, the demand for memory is

greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the memory usage value is high, and the host has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot handle the demand for memory. It leads to memory reclamation, which might degrade performance.

If the host has enough free memory, check the resource shares, reservation, and limit settings of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machines.

If the host has little free memory available, or if you notice a degradation in performance, consider taking the following actions.

Table 372: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory Consumed

The Memory Consumed chart displays memory usage for the 10 child objects in the cluster with the most consumed memory.

For resource pools and virtual machines in a cluster, this chart is located in the **Resource Pools & Virtual Machines** view of the cluster **Performance** tab. For hosts in a cluster, this chart is located in the **Hosts** view of the cluster **Performance** tab.

Table 373: Data Counters

Chart Label	Description
resource_pool, *virtual_machine*, or *host*	Amount of machine memory used by all resource pools and virtual machines in the cluster or by all hosts in the cluster, depending on the cluster view. Consumed memory includes virtual machine memory, service console memory, and VMkernel memory. consumed memory = total host memory - free host memory • Counter: consumed • Stats Type: Absolute • Unit: MegaBytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Memory usage is not necessarily an indicator of performance problems. Memory can be high if a host is swapping or ballooning, which can result in virtual machine guest swapping. In such cases, check for other problems, such as CPU over-commitment or storage latencies.

If you have constantly high memory usage in a cluster, resource pool, or vApp, consider taking the following actions.

Table 374: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	Verify that the balloon driver is enabled. The balloon driver is installed with VMware Tools and is critical to performance. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.
3	If the balloon value is high, check the resource shares, reservations, and limits for the virtual machines and resource pools on the hosts. Verify that the host's settings are adequate and not lower than those set for the virtual machine. If free memory is available on the hosts and the virtual machines are experiencing high swap or balloon memory, the virtual machine (or resource pool, if it belongs to one) has reached its resource limit. Check the maximum resource limit set on that host.
4	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
5	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. It might help avoid hot spots in the cluster.
6	Add more physical memory to one or more hosts.

Network (Mbps)

The Network (Mbps) chart displays network speed for the 10 hosts in the cluster with the most network usage.

This chart is located in the **Hosts** view of the Cluster **Performance** tab.

Table 375: Data Counters

Chart Label	Description
<host>	Average rate at which data is transmitted and received across all NIC instances on the host. • Counter: usage • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 376: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Data centers

The data center charts contain information about CPU, disk, memory, and storage usage for data centers. The help topic for each chart contains information about the data counters displayed in that chart. The counters available are determined by the collection level set for vCenter Server.

CPU (MHz)

The CPU (MHz) chart displays CPU usage for the 10 clusters in the data center with the most CPU usage.

This chart is located in the Clusters view of the Datacenters **Performance** tab.

Table 377: Data Counters

Chart Label	Description
<cluster>	Amount of CPU currently in use by the cluster. The active CPU usage is approximately equal to the ratio of the used CPU cycles to the available CPU cycles. The maximum possible value is the frequency of the processors multiplied by the number of cores. For example, a two-way SMP virtual machine using 4000MHz on a host that has four 2GHz processors is using 50% of the CPU (4000 ÷ 4 × 2000) = 0.5). • Counter: usagemhz • Stats Type: Rate • Unit: MegaHertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of cluster resources. However, if the value is constantly high, the CPU demanded is likely greater than the CPU capacity available. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the hosts in the cluster.

If performance is impacted, consider taking the following actions.

Table 378: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
3	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. This might help avoid hot spots in the cluster.
4	Migrate one or more virtual machines to a new host.
5	Upgrade the physical CPUs or cores on each host in the cluster if necessary.
6	Enable CPU-saving features, such as TCP Segmentation Offload.
7	Replace software I/O with the dedicated hardware, such as iSCSI HBAs or TCP Segmentation Offload NICs.

Memory (MB)

The Memory (MB) chart displays the average amount of consumed memory for the 10 clusters in the data center with the most consumed memory.

This chart is located in the **Clusters** view of the Datacenters **Performance** tab.

Table 379: Data Counters

Chart Label	Description
<cluster>	Amount of host machine memory used by all powered on virtual machines in the cluster. • Counter: consumed • Stats Type: Absolute • Unit: MegaBytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A cluster's consumed memory consists of virtual machine consumed memory and overhead memory. It does not include host-specific overhead memory, such as memory used by the service console or VMkernel.

If you experience problems with cluster memory usage, use the thumbnail cluster charts to examine memory usage for each cluster and increase memory resources if needed.

If the cluster is a DRS cluster, check the aggressiveness threshold. If the value is low, increase the threshold. Increasing the threshold might help avoid hot spots in the cluster.

Space Utilization By File Type

The Space Utilization By File Type chart displays datastore space usage for virtual disks, swap files, snapshot files, and other virtual machine files.

Note: This chart does not show historical statistics. It only shows the most recently available data, which may be up to 30 minutes late, depending on when the last statistics rollup occurred. In addition, statistics are not collected across all datastores at one time. They are collected asynchronously.

The Space Utilization by File Type chart is located in the **Storage** view of the data center **Performance** tab.

Datastore Counters

Table 380: Data Counters

File Type	Description
Virtual Disks	Amount of disk space used by virtual disk files. Virtual disk files store the contents of the virtual machine's hard disk drive. It includes information that you write to a virtual machine's hard disk, such as the operating system, program files, and data files. The files have the extension `.vmdk` and appear as a physical disk drive to a guest operating system. **Note:** Delta disks, which also have an extension `.vmdk`, are not included in this file type. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB)

File Type	Description
	• Rollup Type: Latest • Collection Level: 1 (4)
Swap Files	Amount of disk space used by swap files. Swap files back up the virtual machine's physical memory. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Snapshots	Amount of disk space used by virtual machine snapshot files. Snapshot files store information about virtual machine snapshots. They include snapshot state files and delta disk files. A snapshot state file stores the running state of the virtual machine at the time of the snapshot. It has the extension `.vmsn`. A delta disk file stores the updates made by the virtual machine to the virtual disks after a snapshot is taken. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Other VM Files	Amount of disk space used by all other virtual machine files, such as configuration files and log files. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Other	Amount of disk space used by all other non-virtual machine files, such as documentation files and backup files.
Free Space	Amount of disk space not currently in use.
Total Space	Amount of disk space available to the datastore. It defines the datastore capacity. The chart displays the information for datastores but not for data centers. total space = virtual disk space + swap file space + snapshot space + other VM file space + other space + free space

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Datastores and Datastore Clusters

The datastore charts contain information about disk usage for datastores or the datastores that are part of a cluster. The help topic for each chart contains information about the data counters displayed in that chart. The counters available are determined by the collection level set for vCenter Server.

Space in GB

The Space in GB chart displays space usage data counters for datastores.

This chart is located in the **Space** view of the datastore or datastore cluster **Performance** tab.

Table 381: Data Counters

Chart Label	Description
Allocated	Amount of physical space provisioned by an administrator for the datastore. It is the storage size up to which files on the datastore can grow. Allocated space is not always in use. • Counter: provisioned • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1
Used	Amount of physical datastore space in use. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1
Capacity	Maximum capacity of the datastore. capacity = virtual machine file space + non-virtual machine file space + free space **Note:** Storage data is collected and updated in the overview charts every 30 minutes. Therefore, if you refresh the datastore, the capacity value might only be updated in the datastore **Summary** tab, and not in the overview charts. • Counter: capacity • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space Utilization By File Type

The Space Utilization by File Type chart displays space used by virtual disks, swap files, snapshot files, and other virtual machine files on the datastore or the datastore cluster.

Note: This chart does not show historical statistics. It only shows the most recently available data, which may be up to 30 minutes late, depending on when the last statistics rollup occurred. In addition, statistics are not collected across all datastores at one time. They are collected asynchronously.

The Space Utilization by File Type chart is located in the **Storage** view of the datastore **Performance** tab. The counters can also be displayed for datastore cluster charts.

Datastore Counters

Table 382: Data Counters

File Type	Description
Virtual Disks	Amount of disk space used by virtual disk files. Virtual disk files store the contents of the virtual machine's hard disk drive. It includes information that you write to a virtual machine's hard disk, such as the operating system, program files, and data files. The files have the extension `.vmdk` and appear as a physical disk drive to a guest operating system. **Note:** Delta disks, which also have an extension `.vmdk`, are not included in this file type. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Swap Files	Amount of disk space used by swap files. Swap files back up the virtual machine's physical memory. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Snapshots	Amount of disk space used by virtual machine snapshot files. Snapshot files store information about virtual machine snapshots. They include snapshot state files and delta disk files. A snapshot state file stores the running state of the virtual machine at the time of the snapshot. It has the extension `.vmsn`. A delta disk file stores the updates made by the virtual machine to the virtual disks after a snapshot is taken. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Other VM Files	Amount of disk space used by all other virtual machine files, such as configuration files and log files. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Other	Amount of disk space used by all other non-virtual machine files, such as documentation files and backup files.
Free Space	Amount of disk space not currently in use.
Total Space	Amount of disk space available to the datastore. It defines the datastore capacity. The chart displays the information for datastores but not for data centers. total space = virtual disk space + swap file space + snapshot space + other VM file space + other space + free space

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space used by Datastore in GB

The Space used by Datastore in GB chart displays the 10 datastores in the data center with the most used disk space.

This chart is located in the **Storage** view of the Datacenter **Performance** tab.

Table 383: Data Counters

Chart Label	Description
<datastore>	Amount of used storage space on the 10 datastores with the most used space. • Counter: used • Stats Type: Absolute • Unit: GigaBytes (GB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space Utilization by Virtual Machine

The Space Utilization by Virtual Machine chart displays the amount of space used by the five virtual machines with the most space used on the datastore or the datastores in the cluster.

Note: This chart does not show historical statistics. It only shows the most recently available data, which may be up to 30 minutes late, depending on when the last statistics rollup occurred. In addition, statistics are not collected across all datastores at one time. They are collected asynchronously.

The Space Utilization by Virtual Machine chart is located in the **Space** view of the datastore **Performance** tab. The counter can also be displayed for datastore cluster charts.

Table 384: Data Counters

Chart Label	Description
virtual_machine	Amount of datastore space used by the five virtual machines with the most used datastore space.

Chart Label	Description
	• Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space Allocated by Datastore in GB

The Space allocated by Datastore in GB displays the top 10 datastores, virtual machines in the datastore-cluster with most provisioned space.

This chart is located in the **Space** view of the Datacenter **Performance** tab.

Table 385: Data Counters

Chart Label	Description
<datastore>	Amount of provisioned storage space on the top 10 datastores with the most provisioned space. • Counter: provisioned • Stats Type: Absolute • Unit: KiloBytes (KB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space Capacity by Datastore in GB

The Space capacity by Datastore in GB displays the top 10 configured size of the datastores in the datastore cluster.

This chart is located in the **Space** view of the Datacenter **Performance** tab.

Table 386: Data Counters

Chart Label	Description
<datastore>	Configured size of the datastores in the datastore cluster. • Counter: capacity • Stats Type: Absolute • Unit: KiloBytes (KB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Storage I/O Control Normalized Latency

This chart displays the normalized latency in microseconds on the datastore. Storage I/O Control monitors latency to detect congestion on the datastore. This metric computes a weighted response time across all hosts and VMs accessing the datastore. I/O count is used as the weight for the response time. It captures the device level latency and does not include any queuing inside the hypervisor storage stack or inside the VM. It is adjusted for the I/O size. High latencies that are the result of large I/Os are discounted so as not to make the datastore seem slower than it really is. Data for all virtual machines is combined. This chart displays zero values when Storage I/O Control is disabled.

This chart is located in the **Performance** view of the datastore **Performance** tab. The sizeNormalizedDatastoreLatency counter can also be displayed for datastore cluster charts.

Table 387: Data Counters

Chart Label	Description
Storage I/O Control Normalized Latency	Storage I/O Control monitors latency to detect congestion on the datastore. • Counter: sizeNormalizedDatastoreLatency • Stats Type: Absolute • Unit: Microseconds • Rollup Type: Average • Collection Level: 3

Storage I/O Control Aggregate IOPs

This chart displays the number of I/O operations per one second on the datastore, aggregated across all hosts, and virtual machines accessing this datastore. The chart displays zero values when Storage I/O Control is disabled.

This chart is located in the **Performance** view of the datastore or the datastore cluster **Performance** tab. The counter can be displayed for datastore and datastore cluster charts.

Table 388: Data Counters

Chart Label	Description
Storage I/O Control Aggregate IOPs	Number of I/O operations per second on the datastore, aggregated across all hosts, and virtual machines accessing the datastore. • Counter: datastoreIops • Stats Type: Absolute • Unit: Number • Rollup Type: Average • Collection Level: 3

Storage I/O Control Activity

This chart displays the percentage of time during which Storage I/O Control actively controlled latency of the datastore.

This chart is located in the **Performance** views of the datastore **Performance** tabs. The counter can also be displayed for datastore cluster charts.

Table 389: Data Counters

Chart Label	Description
Storage I/O Control Activity	This is the percentage of time during which the Storage I/O Control actively controlled the I/O latency for the datastore. • Counter: siocActiveTimePercentage • Stats Type: Absolute • Unit: Percent • Rollup Type: Average • Collection Level: 3

Average Device Latency per Host

This chart displays the average amount of latency on a host device. The chart displays the 10 hosts with the highest device latency.

This chart is located in the **Performance** view of the datastore **Performance** tab.

Table 390: Data Counters

Chart Label	Description
Average Device Latency per Host	Measures the amount of time, in milliseconds, to complete a SCSI command issued from the physical device. • Counter: deviceLatency • Stats Type: Absolute • Unit: Milliseconds (ms) • Rollup Type: Average • Collection Level: 3

Maximum Queue Depth per Host

This chart displays maximum queue depth that hosts are currently maintaining for the datastore. When Storage I/O is enabled, queue depth can change over time when congestion is detected at the array.

This chart is located in the **Performance** view of the datastore **Performance** tab. The chart displays information about the ten hosts with the highest values.

Table 391: Data Counters

Chart Label	Description
Max Queue Depth per Host	Maximum queue depth. Queue depth is the number of commands the SCSI driver queues to the HBA. • Counter: maxQueueDepth • Stats Type: Absolute • Unit: Number • Rollup Type: Average • Collection Level: 3

Read IOPs per Host

This chart displays the per-host disk read rates for a datastore. The chart displays information about the ten hosts with the highest values.

This chart is located in the **Performance** view of the datastore **Performance** tab.

Table 392: Data Counters

Chart Label	Description
Read IOPs per Host	Number of disk read commands completed on each disk on the host, per second. Read rate = blocks read per second × block size • Counter: numberReadAveraged • Stats Type: Rate • Unit: Number • Rollup Type: Average • Collection Level: 3

Write IOPs Per Host

This chart displays the per-host disk write rates for a datastore. The chart displays information about the 10 hosts with the highest values.

This chart is located in the **Performance** view of the datastore **Performance** tab.

Table 393: Data Counters

Chart Label	Description
Write IOPs per Host	Number of disk write commands completed on each disk on the host, per second. Write rate = blocks written per second × block size • Counter: numberWriteAveraged

Chart Label	Description
	• Stats Type: Rate • Unit: Number • Rollup Type: Average • Collection Level: 3

Average Read Latency per Virtual Machine Disk

This chart displays the top ten virtual machine disks with the highest average read latency in milliseconds. Data is not displayed when the virtual machine is powered off.

This chart is located in the **Performance** view of the datastore **Performance** tab. The counter can also be displayed for datastore cluster charts.

Table 394: Data Counters

Chart Label	Description
Average Read Latency per Virtual Machine Disk	Latency measures the time used to process a SCSI command issued by the guest OS to the virtual machine. The kernel latency is the time VMkernel takes to process an I/O request. The device latency is the time it takes the hardware to handle the request. Total latency = kernelLatency + deviceLatency. • Counter: totalReadLatency • Stats Type: Absolute • Unit: Milliseconds (ms) • Rollup Type: Average • Collection Level: 3

Average Write Latency per Virtual Machine Disk

This chart displays the top ten virtual machine disks with the highest average write latency in milliseconds. Data is not displayed when the virtual machine is powered off.

This chart is located in the **Performance** view of the datastore **Performance** tab. The counter can also be displayed for datastore cluster charts.

Table 395: Data Counters

Chart Label	Description
Average Write Latency per Virtual Machine Disk	Latency measures the time used to process a SCSI command issued by the guest OS to the virtual machine. The kernel latency is the time VMkernel takes to process an I/O request. The device latency is the time it takes the hardware to handle the request. Total latency = kernelLatency + deviceLatency. • Counter: totalWriteLatency • Stats Type: Absolute • Unit: Milliseconds (ms) • Rollup Type: Average • Collection Level: 3

Read IOPs per Virtual Machine Disk

This chart displays the top ten virtual machines with the highest number of read operations. Data is not displayed when the virtual machine is powered off.

This chart is located in the **Performance** view of the datastore **Performance** tab. The counter can also be displayed for datastore cluster charts.

Table 396: Data Counters

Chart Label	Description
Read IOPs per Virtual Machine Disk	Number of disk read commands completed on each virtual machine disk, per second. Read rate = blocks read per second × block size • Counter: numberReadAveraged • Stats Type: Rate • Unit: Number • Rollup Type: Average • Collection Level: 3

Write IOPs Per Virtual Machine Disk

This chart displays the 10 virtual machines with the highest number of write operations. Data is not displayed when the virtual machine is powered off.

This chart is located in the **Performance** view of the datastore **Performance** tab. The counter can also be displayed for datastore cluster charts.

Table 397: Data Counters

Chart Label	Description
Write IOPs per Virtual Machine Disk	Number of disk write commands completed on each virtual machine disk on the host. Write rate = blocks read per second × block size • Counter: numberWriteAveraged • Stats Type: Rate • Unit: Number • Rollup Type: Average • Collection Level: 3

Virtual Machine Observed Latency per Datastore

This chart displays the average datastore latency as observed by the virtual machines.

This chart is located in the **Performance** view of the datastore cluster **Performance** tab.

Table 398: Data Counters

Chart Label	Description
VM observed latency report per Datastore	This is the average datastore latency as observed by the virtual machines in the datastore cluster. • Counter: datastoreVMObservedLatency

Chart Label	Description
	• Stats Type: Absolute • Unit: Microseconds • Rollup Type: Latest • Collection Level: 3

Hosts

The hosts charts contain information about CPU, disk, memory, network, and storage usage for hosts. The help topic for each chart contains information about the data counters displayed in that chart. The counters available are determined by the collection level set for vCenter Server.

CPU (%)

The CPU (%) chart displays CPU usage for the host.

This chart is located in the Home view of the Host **Performance** tab.

Table 399: Data Counters

Chart Label	Description
Usage	Actively used CPU, as a percentage of the total available CPU, for each physical CPU on the host. Active CPU is approximately equal to the ratio of the used CPU to the available CPU. Available CPU = # of physical CPUs × clock rate. 100% represents all CPUs on the host. For example, if a four-CPU host is running a virtual machine with two CPUs, and the usage is 50%, the host is using two CPUs completely. • Counter: usage • Stats Type: Rate • Unit: Percentage (%) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of the host resources. However, if the value is constantly high, the host is probably lacking the CPU required to meet the demand. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the host.

If performance is impacted, consider taking the following actions.

Table 400: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.

#	Resolution
4	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
5	Upgrade the physical CPUs or cores on the host if necessary.
6	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

CPU (MHz)

The CPU (MHz) chart displays CPU usage for the host.

This chart is located in the Home view of the Host **Performance** tab.

Table 401: Data Counters

Chart Label	Description
Usage	The sum, in megahertz, of the actively used CPU of all powered on virtual machines on a host. The maximum possible value is the frequency of the processors multiplied by the number of processors. For example, if you have a host with four 2GHz CPUs running a virtual machine that is using 4000MHz, the host is using two CPUs completely. 4000 ÷ (4 × 2000) = 0.50 • Counter: usagemhz • Stats Type: Rate • Unit: MegaHertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of the host resources. However, if the value is constantly high, the host is probably lacking the CPU required to meet the demand. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the host.

If performance is impacted, consider taking the following actions.

Table 402: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
4	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
5	Upgrade the physical CPUs or cores on the host if necessary.

#	Resolution
6	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

CPU Usage

The CPU Usage chart displays CPU usage of the 10 virtual machines on the host with the most CPU usage.

This chart is located in the Virtual Machines view of the host **Performance** tab.

Table 403: Counters

Name	Description
virtual_machine	Amount of CPU actively being used by each virtual machine on the host. 100% represents all CPUs. For example, if a virtual machine has one virtual CPU that is running on a host with four CPUs and the CPU usage is 100%, the virtual machine is using one CPU resource. virtual CPU usage = usagemhz ÷ (number of virtual CPUs × core frequency) **Note:** The host's view of the CPU usage, not the guest operating system view. • Counter: usage • Stats Type: Rate • Unit: Percentage (%). Precision is to 1/100%. A value between 0 and 100. • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage or CPU ready indicates that you are making the best use of the virtual machine resources. However, if the CPU usage value for a virtual machine is above 90% and the CPU ready value is above 20%, performance is being impacted.

If performance is impacted, consider taking the following actions.

Table 404: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked line chart on the host's **Virtual Machine** view shows the CPU usage for virtual machines on the host.
4	Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
5	Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
6	Increase the amount of memory allocated to the virtual machine. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.

#	Resolution
7	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
8	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
9	Upgrade the physical CPUs or cores on the host if necessary.
10	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Disk (KBps)

The Disk (KBps) chart displays disk I/O of the host.

This chart is located in the Home view of the host **Performance** tab.

Table 405: Data Counters

Chart Label	Description
Usage	Average data I/O rate across all LUNs on the host. • Counter: usage • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 406: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Disk Rate (KBps)

The Disk Rate chart displays disk read and write rates for LUNs on a host, including average rates.

This chart is located in the **Home** view of the host **Performance** tab.

Table 407: Data Counters

Chart Label	Description
Read	Number of disk read commands completed on each disk on the host, per second. The aggregate number of all disk read commands is also displayed in the chart. Read rate = blocksRead per second × blockSize • Counter: read • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average • Collection Level: 3

Chart Label	Description
Write	Number of disk write commands completed on each disk on the host, per second. The aggregate number of all disk write commands is also displayed in the chart. Write rate = blocksWritten per second × blockSize • Counter: write • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average • Collection Level: 3

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 408: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.

#	Resolution
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Disk Requests (Number)

The Disk Requests chart displays disk usage for the host.

This chart is located in the **Home** view of the host **Performance** tab.

Table 409: Data Counters

Chart Label	Description
Read Requests	Number of disk read commands completed on each LUN on the host. The aggregate number of all disk read commands is also displayed in the chart. • Counter: numberRead • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3
Write Requests	Number of disk write commands completed on each LUN on the host. The aggregate number of all disk write commands is also displayed in the chart. • Counter: numberWrite • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.

- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 410: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Disk (Number)

The Disk (Number) chart displays maximum queue depth for the top ten LUNs on a host.

This chart is located in the **Home** view of the host **Performance** tab.

Table 411: Data Counters

Chart Label	Description
Maximum Queue Depth	Maximum queue depth. Queue depth is the number of commands the SCSI driver queues to the HBA. • Counter: maxQueueDepth • Stats Type: Absolute • Unit: Number • Rollup Type: Average • Collection Level: 1

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 412: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.

#	Resolution
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Disk (ms)

The Disk (ms) chart displays the amount of time taken to process commands on a host.

This chart is located in the **Home** view of the host **Performance** tab.

Table 413: Data Counters

Chart Label	Description
Highest Disk Latency	Highest latency value of all disks used by the host. Latency measures the time used to process a SCSI command issued by the guest OS to the virtual machine. The kernel latency is the time VMkernel takes to process an I/O request. The device latency is the time it takes the hardware to handle the request. Total latency = kernelLatency + deviceLatency. • Counter: maxTotalLatency • Stats Type: Absolute • Unit: Milliseconds (ms) • Rollup Type: Latest (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.

- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 414: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Disk (KBps)

The Disk (KBps) chart displays disk usage for the 10 virtual machines on the host with the most disk usage.

This chart is located in the **Virtual Machines** view of the host **Performance** tab.

Table 415: Data Counters

Chart Label	Description
virtual_machine	Sum of the data read from the virtual machine. • Counter: usage • Stats Type: Rate • Unit: KiloBytes per second (KBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 416: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.

#	Resolution
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Memory (%)

The Memory (%) chart displays host memory usage.

This chart is located in the **Home** view of the host **Performance** tab.

Chart Analysis

To ensure best performance, the host memory must be large enough to accommodate the active memory of the virtual machines. The active memory can be smaller than the virtual machine memory size. It allows you to over-provision memory, but still ensures that the virtual machine active memory is smaller than the host memory.

Transient high-usage values usually do not cause performance degradation. For example, memory usage can be high when several virtual machines are started at the same time or when a spike occurs in virtual machine workload. However, a consistently high memory usage value (94% or greater) indicates that the host is probably lacking the memory required to meet the demand. If the active memory size is the same as the granted memory size, the demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the memory usage value is high, and the host has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot handle the demand for memory. It leads to memory reclamation, which might degrade performance.

If the host has enough free memory, check the resource shares, reservation, and limit settings of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machines.

If the host has little free memory available, or if you notice a degradation in performance, consider taking the following actions.

Table 417: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.

#	Resolution
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory (Balloon)

The Memory (Balloon) chart displays balloon memory on a host.

This chart is located in the **Home** view of the host **Performance** tab.

Table 418: Data Counters

Chart Label	Description
Balloon	Sum of the guest physical memory reclaimed by the balloon driver for all powered on virtual machines on the host. • Counter: vmmemctl • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

To ensure best performance, the host memory must be large enough to accommodate the active memory of the virtual machines. The active memory can be smaller than the virtual machine memory size. It allows you to over-provision memory, but still ensures that the virtual machine active memory is smaller than the host memory.

Transient high-usage values usually do not cause performance degradation. For example, memory usage can be high when several virtual machines are started at the same time or when a spike occurs in virtual machine workload. However, a consistently high memory usage value (94% or greater) indicates that the host is probably lacking the memory required to meet the demand. If the active memory size is the same as the granted memory size, the demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the memory usage value is high, and the host has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot handle the demand for memory. It leads to memory reclamation, which might degrade performance.

If the host has enough free memory, check the resource shares, reservation, and limit settings of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machines.

If the host has little free memory available, or if you notice a degradation in performance, consider taking the following actions.

Table 419: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory (MBps)

The Memory (MBps) chart displays the swap in and swap out rates for a host.

This chart is located on the **Home** view of the Host **Performance** tab.

Table 420: Data Counters

Chart Label	Description
swapinRate	Average rate at which memory is swapped in from the host swap file. • Counter: swapinRate • Stats Type: Rate • Unit: MegaBytes per second (MBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
swapoutRate	Average rate at which memory is swapped out to the host swap file. • Counter: swapoutRate • Stats Type: Rate • Unit: MegaBytes per second (MBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Host memory must be large enough to accommodate virtual machine workload. Transient high-usage values usually do not cause performance degradation. For example, memory usage can be high when several virtual machines are started at the same time or when there is a spike in virtual machine workload.

However, a consistently high memory usage value (94% or greater) indicates the host does not have the memory resources required to meet the demand. If the memory balloon and swap values are not high, performance is probably not affected. If the memory usage value is high, and the host has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host requires more memory resources.

If the host is not lacking memory resources, check the resource shares, reservation, and limit settings of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machines.

If the host is lacking memory resources or you notice a degredation in performance, consider taking the following actions.

Table 421: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of a virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory (MB)

The Memory (MB) chart displays memory data counters for hosts.

This chart is located in the **Home** view of the host **Performance** tab.

Note: Guest physical memory refers to the virtual hardware memory presented to a virtual machine for its guest operating system. Machine memory is the actual physical RAM in the host.

Not all counters are collected at collection level 1.

Table 422: Data Counters

Chart Label	Description
Active	Sum of the active guest physical memory of all powered on virtual machines on the host, plus memory used by basic VMKernel applications. Active memory is estimated by the VMkernel and is based on the current workload of the host. • Counter: active • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Balloon	Sum of the guest physical memory reclaimed by the balloon driver for all powered on virtual machines on the host. • Counter: vmmemctl • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Label	Description
Balloon Target	Sum of the balloon target memory of all powered on virtual machines on the host. If the balloon target value is greater than the balloon value, the VMkernel inflates the balloon, causing more virtual machine memory to be reclaimed. If the balloon target value is less than the balloon value, the VMkernel deflates the balloon, which allows the virtual machine to consume additional memory if needed. Virtual machines initiate memory reallocation. Therefore, it is possible to have a balloon target value of 0 and a balloon value greater than 0. • Counter: vmmemctltarget • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Consumed	Amount of machine memory used on the host. Consumed memory includes virtual machine memory, service console memory, and VMkernel memory. consumed memory = total host memory - free host memory • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Granted	Sum of the guest physical memory granted for all powered on virtual machines. Granted memory is mapped to the host's machine memory. Granted memory for a host includes the shared memory of each virtual machine on the host. • Counter: granted • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Shared Common	Amount of machine memory shared by all powered on virtual machines. Shared common memory consists of the entire pool of memory from which sharing is possible, including the amount of physical RAM required by the guest memory. memory shared - memory shared common = amount of memory saved on the host from sharing • Counter: sharedcommon • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Swap Used	Sum of the memory swapped by all powered on virtual machines on the host. • Counter: swapused • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)

Chart Analysis

To ensure best performance, the host memory must be large enough to accommodate the active memory of the virtual machines. The active memory can be smaller than the virtual machine memory size. It allows you to over-provision memory, but still ensures that the virtual machine active memory is smaller than the host memory.

Transient high-usage values usually do not cause performance degradation. For example, memory usage can be high when several virtual machines are started at the same time or when a spike occurs in virtual machine workload. However, a consistently high memory usage value (94% or greater) indicates that the host is probably lacking the memory required to meet the demand. If the active memory size is the same as the granted memory size, the demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the memory usage value is high, and the host has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot handle the demand for memory. It leads to memory reclamation, which might degrade performance.

If the host has enough free memory, check the resource shares, reservation, and limit settings of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machines.

If the host has little free memory available, or if you notice a degradation in performance, consider taking the following actions.

Table 423: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory Usage

The Memory Usage chart displays memory usage for the 10 virtual machines on the host with the most memory usage.

This chart is located in the **Virtual Machines** view of the host **Performance** tab.

Virtual Machine Counters

Note: Guest physical memory refers to the virtual hardware memory presented to a virtual machine for its guest operating system.

Table 424: Data Counters

Chart Label	Description
Usage	Amount of guest physical memory currently in use on the virtual machine. • Counter: usage • Stats Type: Absolute • Unit: Percentage (%) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 425: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory Bandwidth (MBps)

The Memory Bandwidth chart displays DRAM and/or PMem Bandwidth graphs of the host.

This chart is available in the **Memory** pane of the **View** dropdown menu of vSphere Client for a host instance at **Performance** > **Overview** tab. The Memory pane gives information about Memory Bandwidth in addition to the Memory Utilization and Memory Reclamation information. It also gives the Memory Miss Rate, but only in Memory mode.

Note: PMem Bandwidth is only available on supported hosts configured in Memory Mode. If the host is not supported by vMMR, then the **Memory** option is not listed in the **View** dropdown menu.

Table 426: Data Counters

Chart Label	Description
Estimated DRAM Bandwidth	Total read and write bandwidth of the DRAM memory type. • Counter: bandwidth.total • Stats Type: Absolute • Unit: MegaBytes per second (MBps) • Rollup Type: Latest • Collection Level: 1 (4)
Estimated PMem Bandwidth	Total read and write bandwidth of the PMem memory type. • Counter: bandwidth.total • Stats Type: Absolute • Unit: MegaBytes per second (MBps) • Rollup Type: Latest • Collection Level: 1 (4)

Memory Miss Rate (%)

The Memory Miss Rate performance chart displays DRAM Miss Rate graph for the host.

This chart is available in the **Memory** pane of the **View** dropdown menu of vSphere Client for a host instance at **Performance** > **Overview** tab. The Memory pane gives information about Memory Miss Rate (DRAM) in addition to the memory consumption, memory reclamation, and memory bandwidth information.

Note: Miss rate is only supported on supported hosts in Memory Mode. If the host is not supported by vMMR, then the **Memory** option is not listed in the **View** dropdown menu.

Table 427: Data Counters

Chart Label	Description
Estimated DRAM Miss Rate	Get the current miss rate of DRAM memory type. • Counter: missrate • Stats Type: Absolute • Unit: % • Rollup Type: Latest • Collection Level: 2 (4)

Network (Mbps)

The Network (Mbps) chart displays network usage for the host.

This chart is located in the **Home** view of the Host **Performance** tab.

Table 428: Host Counters

Chart Label	Description
Usage	Average rate at which data is transmitted and received across all NIC instances connected to the host. • Counter: usage • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 429: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.

#	Resolution
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Network Rate (Mbps)

The Network Rate chart displays network bandwidth on a host.

The Network Data Transmitted/Received chart for hosts is located in the **Home** view of the Host **Performance** tab.

Table 430: Data Counters

Chart Label	Description
Data Receive Rate	Rate at which data is received across the top ten physical NIC instances on the host. This represents the bandwidth of the network. The chart also displays the aggregated data receive rate of all physical NICs. • Counter: received • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average • Collection Level: 3 (4)
Data Transmit Rate	Rate at which data is transmitted across the top ten physical NIC instances on the host. This represents the bandwidth of the network. The chart also displays the aggregated data transmit rate of all physical NICs. • Counter: transmitted • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average • Collection Level: 3 (4)

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform

load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 431: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Network Packets (Number)

The Network Packets chart displays the network bandwidth on a host.

This chart is located in the **Home** view of the Host **Performance** tab.

Table 432: Data Counters

Chart Label	Description
Packets Received	Number of network packets received across the top ten physical NIC instances on the host. The chart also displays the aggregated value for all NICs. • Counter: packetRx • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3
Packets Transmitted	Number of network packets transmitted across the top ten physical NIC instances on the host. The chart also displays the aggregated value for all NICs. • Counter: packetTx • Stats Type: Absolute • Unit: Number

Chart Label	Description
	• Rollup Type: Summation • Collection Level: 3

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 433: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Network (Mbps)

The Network (Mbps) chart displays network usage for the 10 virtual machines on the host with the most network usage.

This chart is located in the **Virtual Machines** view of the host **Performance** tab.

Table 434: Data Counters

Chart Label	Description
<virtual machine>	Sum of the data transmitted and received across all virtual NIC instances connected to the virtual machine. • Counter: usage • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 435: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.

#	Resolution
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Resource Pools

The resource pool charts contain information about CPU and memory usage for resource pools. The help topic for each chart contains information about the data counters displayed in that chart. The counters available are determined by the collection level set for vCenter Server.

CPU (MHz)

The CPU (MHz) chart displays CPU usage in the resource pool or vApp.

This chart is located in the Home view of the Resource Pool or vApp **Performance** tab.

Counters

Table 436: Data Counters

Chart Label	Description
Usage	CPU usage is the sum of the average CPU usage values of the virtual machines in the resource pool or vApp. CPU usage = number of cores * CPU frequency • Counter: usagemhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of the resources available. However, if the value is constantly high, the CPU demanded is likely greater than the CPU capacity available. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines in the resource pool. Generally, if the CPU usage value for a virtual machine is above 90% and the CPU ready value for a virtual machine is above 20%, performance is impacted.

If performance is impacted, consider taking the following actions.

Table 437: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	Deploy single-threaded applications on uniprocessor virtual machines instead of SMP virtual machines.
3	Migrate one or more virtual machines to a new host.
4	Upgrade the physical CPUs or cores on each host if necessary.
5	Enable CPU-saving features, such as TCP Segmentation Offload.
6	Replace software I/O with dedicated hardware, such as iSCSI HBAs or TCP Segmentation Offload NICs.

CPU Usage

The CPU Usage chart displays CPU usage of virtual machines in the resource pool or vApp. The chart displays the top 10 virtual machines with the highest CPU usage.

This chart is located in the Resource Pools & Virtual Machines view of the Resource Pool or vApp **Performance** tab.

Table 438: Data Counters

Chart Label	Description
virtual_machine	Amount of CPU actively used by virtual machines. • Counter: usagemhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage or CPU ready indicates that you are making the best use of the virtual machine resources. However, if the CPU usage value for a virtual machine is above 90% and the CPU ready value is above 20%, performance is being impacted.

If performance is impacted, consider taking the following actions.

Table 439: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked line chart on the host's **Virtual Machine** view shows the CPU usage for virtual machines on the host.
4	Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.

#	Resolution
5	Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
6	Increase the amount of memory allocated to the virtual machine. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
7	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
8	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
9	Upgrade the physical CPUs or cores on the host if necessary.
10	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Memory (MB)

The Memory (MB) chart displays memory usage in the resource pool or vApp.

This chart is located in the **Home** view of the resource pool or vApp **Performance** tab.

Table 440: Data Counters

Chart Label	Description
resource_pool or *vApp*	Sum of the active memory used by all virtual machines in the resource pool or vApp. Active memory is determined by the VMkernel and includes overhead memory. memory usage = active memory / configured virtual machine memory size • Counter: used • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average • Collection Level: 1

Chart Analysis

Memory usage is not necessarily an indicator of performance problems. Memory can be high if a host is swapping or ballooning, which can result in virtual machine guest swapping. In such cases, check for other problems, such as CPU over-commitment or storage latencies.

If you have constantly high memory usage in a cluster, resource pool, or vApp, consider taking the following actions.

Table 441: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.

#	Resolution
2	Verify that the balloon driver is enabled. The balloon driver is installed with VMware Tools and is critical to performance. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.
3	If the balloon value is high, check the resource shares, reservations, and limits for the virtual machines and resource pools on the hosts. Verify that the host's settings are adequate and not lower than those set for the virtual machine. If free memory is available on the hosts and the virtual machines are experiencing high swap or balloon memory, the virtual machine (or resource pool, if it belongs to one) has reached its resource limit. Check the maximum resource limit set on that host.
4	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
5	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. It might help avoid hot spots in the cluster.
6	Add more physical memory to one or more hosts.

Memory Consumed

The Memory Consumed chart displays the memory performance of all virtual machines in the resource pool or vApp.

This chart is located in the **Resource Pools & Virtual Machines** view of the resource pool or vApp **Performance** tab.

For resource pools and virtual machines in a resource pool or vApp, this chart is located in the **Resource Pools & Virtual Machines** view of the resource pool or vApp **Performance** tab.

Table 442: Data Counters

Chart Label	Description
virtual_machine	Amount of host memory used by the virtual machine for its guest operating system's physical memory. Memory overhead is not included in consumed memory. consumed memory = memory granted - memory saved from page sharing For example, if a virtual machine has 100 MB of memory that is shared equally with three other virtual machines, its portion of the shared memory is 25 MB (100 MB ÷ 4 VMs). This amount is counted in the memory consumed data counter. • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 443: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory (MB)

The Memory (MB) chart displays memory data counters for resource pools or vApps.

Description

This chart is located in the **Home** view of the resource pool or vApp **Performance** tab.

Note: These data counter definitions are for virtual machines. At the resource pool level, the values are collected and totaled. The counter values in the chart represent the aggregate amounts of the virtual machine data. The counters that appear in the chart depend on the collection level set for your vCenter Server.

Table 444: Data Counters

Chart Label	Description
Active	Sum of the active guest physical memory of all powered on virtual machines in the resource pool. • Counter: active • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum)

Chart Label	Description
	• Collection Level: 2 (4)
Balloon	Sum of the guest physical memory reclaimed by the balloon driver for all powered on virtual machines in the resource pool. • Counter: vmmemctl • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Consumed	Amount of the physical memory consumed by the virtual machine for the guest memory. Consumed memory does not include the overhead memory. It includes the shared memory and memory that might be reserved, but not actually used. consumed memory = memory granted – memory saved due to memory sharing • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Granted	Sum of the guest physical memory granted for all powered on virtual machines. Granted memory is mapped to the host's machine memory. • Counter: granted • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Shared	Amount of the guest physical memory shared with other virtual machines in the resource pool.
Swapped	Sum of the memory swapped by all powered on virtual machines in the resource pool. • Counter: swapused • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 445: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

vApps

The vApp charts contain information about CPU and memory usage for vApps. The help topic for each chart contains information about the data counters displayed in that chart. The counters available are determined by the collection level set for vCenter Server.

CPU (MHz)

The CPU (MHz) chart displays CPU usage in the vApp or resource pool.

This chart is located in the **Home** view of the vApp or resource pool **Performance** tab.

Counters

Table 446: Data Counters

Chart Label	Description
Usage	CPU usage is the sum of the average CPU usage values of the virtual machines in the resource pool or vApp. CPU usage = number of cores * CPU frequency • Counter: usagemhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage indicates that you are making the best use of the resources available. However, if the value is constantly high, the CPU demanded is likely greater than the CPU capacity available. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines in the resource pool. Generally, if the CPU usage value for a virtual machine is above 90% and the CPU ready value for a virtual machine is above 20%, performance is impacted.

If performance is impacted, consider taking the following actions.

Table 447: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	Deploy single-threaded applications on uniprocessor virtual machines instead of SMP virtual machines.
3	Migrate one or more virtual machines to a new host.
4	Upgrade the physical CPUs or cores on each host if necessary.
5	Enable CPU-saving features, such as TCP Segmentation Offload.
6	Replace software I/O with dedicated hardware, such as iSCSI HBAs or TCP Segmentation Offload NICs.

CPU Usage

The CPU Usage chart displays CPU usage of each virtual machine in the vApp or resource pool.

This chart is located in the **Virtual Machines** view of the vApp or resource pool **Performance** tab.

Table 448: Data Counters

Chart Label	Description
virtual_machine	Amount of CPU actively used by virtual machines. • Counter: usagemhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage or CPU ready indicates that you are making the best use of the virtual machine resources. However, if the CPU usage value for a virtual machine is above 90% and the CPU ready value is above 20%, performance is being impacted.

If performance is impacted, consider taking the following actions.

Table 449: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked line chart on the host's **Virtual Machine** view shows the CPU usage for virtual machines on the host.
4	Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
5	Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.

#	Resolution
6	Increase the amount of memory allocated to the virtual machine. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
7	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
8	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
9	Upgrade the physical CPUs or cores on the host if necessary.
10	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Memory (MB)

The Memory (MB) chart displays memory usage in the vApp or resource pool.

This chart is located in the **Home** view of the vApp or resource pool **Performance** tab.

Table 450: Data Counters

Chart Label	Description
resource_pool or *vApp*	Sum of the active memory used by all virtual machines in the resource pool or vApp. Active memory is determined by the VMkernel and includes overhead memory. memory usage = active memory / configured virtual machine memory size • Counter: used • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average • Collection Level: 1

Chart Analysis

Memory usage is not necessarily an indicator of performance problems. Memory can be high if a host is swapping or ballooning, which can result in virtual machine guest swapping. In such cases, check for other problems, such as CPU over-commitment or storage latencies.

If you have constantly high memory usage in a cluster, resource pool, or vApp, consider taking the following actions.

Table 451: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	Verify that the balloon driver is enabled. The balloon driver is installed with VMware Tools and is critical to performance. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, it does not impact virtual machine performance.

#	Resolution
3	If the balloon value is high, check the resource shares, reservations, and limits for the virtual machines and resource pools on the hosts. Verify that the host's settings are adequate and not lower than those set for the virtual machine. If free memory is available on the hosts and the virtual machines are experiencing high swap or balloon memory, the virtual machine (or resource pool, if it belongs to one) has reached its resource limit. Check the maximum resource limit set on that host.
4	If the cluster is not a DRS cluster, enable DRS. To enable DRS, perform the following tasks: 1. Select the cluster, and click the **Configure** tab. 2. Under **Services**, click **vSphere DRS**. 3. click **Edit**. An Edit Cluster Settings dialog box opens. 4. Click **Turn ON vSphere DRS**, and click **OK**.
5	If the cluster is a DRS cluster: • Increase the number of hosts, and migrate one or more virtual machines to the new host. • Check the aggressiveness threshold. If the value is low, increase the threshold. It might help avoid hot spots in the cluster.
6	Add more physical memory to one or more hosts.

Memory Consumed

The Memory Consumed chart displays the memory performance of the top ten virtual machines in the vApp or resource pool.

This chart is located in the **Virtual Machines** view of the vApp or resource pool **Performance** tab.

For resource pools and virtual machines in a resource pool or vApp, this chart is located in the **Resource Pools & Virtual Machines** view of the resource pool or vApp **Performance** tab.

Table 452: Data Counters

Chart Label	Description
virtual_machine	Amount of host memory used by the virtual machine for its guest operating system's physical memory. Memory overhead is not included in consumed memory. consumed memory = memory granted - memory saved from page sharing For example, if a virtual machine has 100 MB of memory that is shared equally with three other virtual machines, its portion of the shared memory is 25 MB (100 MB ÷ 4 VMs). This amount is counted in the memory consumed data counter. • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 453: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Virtual Machines

The virtual machine charts contain information about CPU, disk, memory, network, storage, and fault tolerance for virtual machines. The help topic for each chart contains information about the data counters displayed in that chart. The counters available are determined by the collection level set for vCenter Server.

CPU (%)

The CPU (%) chart displays virtual machine CPU usage and ready values.

This chart is located in the **Home** view of the virtual machine **Performance** tab.

Table 454: Data Counters

Chart Label	Description
Usage	Amount of actively used virtual CPU as a percentage of total available CPU. CPU usage is the average CPU utilization over all available virtual CPUs in the virtual machine. For example, if a virtual machine with one virtual CPU is running on a host that has four physical CPUs and the CPU usage is 100%, the virtual machine is using one physical CPU completely. virtual CPU usage = usagemhz ÷ (number of virtual CPUs × core frequency) **Note:** This is the host's view of the CPU usage, not the guest operating system view. • Counter: usage • Stats Type: Rate • Unit: Percentage (%). Precision is to 1/100%. A value between 0 and 100. • Rollup Type: Average (Minimum/Maximum)

Chart Label	Description
	• Collection Level: 1 (4)
Ready	Percentage of time that the virtual machine was ready, but could not get scheduled to run on the physical CPU. CPU ready time is dependent on the number of virtual machines on the host and their CPU loads. At collection level 1, the average CPU ready time of all virtual CPUs on the virtual machine is displayed. At collection level 3, the average CPU ready time of each virtual CPU is also displayed. • Counter: ready • Stats Type: Rate • Unit: Percentage (%) • Rollup Type: Summation • Collection Level: 1

Chart Analysis

A short spike in CPU usage or CPU ready indicates that you are making the best use of the virtual machine resources. However, if the CPU usage value for a virtual machine is above 90% and the CPU ready value is above 20%, performance is being impacted.

If performance is impacted, consider taking the following actions.

Table 455: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked line chart on the host's **Virtual Machine** view shows the CPU usage for virtual machines on the host.
4	Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
5	Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
6	Increase the amount of memory allocated to the virtual machine. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
7	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
8	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
9	Upgrade the physical CPUs or cores on the host if necessary.
10	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

CPU Usage (MHz)

The CPU Usage (MHz) chart displays virtual machine CPU usage.

This chart is located in the **Home** view of the Virtual Machine **Performance** tab.

Table 456: Data Counters

Chart Label	Description
Usage	Amount of actively used virtual CPU. **Note:** The host's view of the CPU usage, not the guest operating system view. • Counter: usagemhz • Stats Type: rate • Unit: MegaHertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A short spike in CPU usage or CPU ready indicates that you are making the best use of the virtual machine resources. However, if the CPU usage value for a virtual machine is above 90% and the CPU ready value is above 20%, performance is being impacted.

If performance is impacted, consider taking the following actions.

Table 457: CPU Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on every virtual machine on the host.
2	Set the CPU reservations for all high-priority virtual machines to guarantee that they receive the CPU cycles required.
3	Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked line chart on the host's **Virtual Machine** view shows the CPU usage for virtual machines on the host.
4	Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
5	Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time doesn't decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
6	Increase the amount of memory allocated to the virtual machine. This decreases disk and or network activity for applications that cache. This might lower disk I/O and reduce the need for the host to virtualize the hardware. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
7	Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the hypervisor's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
8	If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
9	Upgrade the physical CPUs or cores on the host if necessary.
10	Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Disk (KBps)

The Disk (KBps) chart displays disk usage for the virtual machine.

It is located in the **Home** view of the virtual machine **Performance** tab.

Table 458: Data Counters

Chart Label	Description
Usage	Average data I/O rate across all virtual disks on the virtual machine. • Counter: usage • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 459: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.

#	Resolution
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Disk Rate (KBps)

The Disk Rate chart displays disk usage for the virtual machine.

This chart is located in the **Home** view of the virtual machine **Performance** tab. It is available only at collection levels 3 and 4.

Table 460: Data Counters

Chart Label	Description
Read	Number of disk read commands completed on each virtual disk on the virtual machine, per second. The aggregate number of all disk read commands per second is also displayed in the chart. Read rate = blocksRead per second × blockSize • Counter: read • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average • Collection Level: 2
Write	Number of disk write commands completed on each virtual disk on the virtual machine, per second. The aggregate number of all disk write commands per second is also displayed in the chart. Write rate = blocksWritten per second × blockSize • Counter: write • Stats Type: Rate • Unit: Kilobytes per second (KBps) • Rollup Type: Average • Collection Level: 2

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 461: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.

#	Resolution
12	Use the most current host hardware.

Disk Requests (Number)

The Disk Requests chart displays disk usage for the virtual machine.

This chart is located in the **Home** view of the virtual machine **Performance** tab. It is available only at collection levels 3 and 4.

Table 462: Data Counters

Chart Label	Description
Read Requests	Number of disk read commands completed on each virtual disk on the virtual machine. The aggregate number of all disk read commands is also displayed in the chart. • Counter: numberRead • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3
Write Requests	Number of disk write commands completed on each virtual disk on the virtual machine. The aggregate number of all disk write commands is also displayed in the chart. • Counter: numberWrite • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3

Chart Analysis

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read or write requests, check whether any such applications were running then.

The best ways to determine if your vSphere environment is experiencing disk problems is to monitor the disk latency data counters. You can use the advanced performance charts to view these statistics.

- The kernelLatency data counter measures the average amount of time, in milliseconds, that the VMkernel spends processing each SCSI command. For best performance, the value must be 0 -1 milliseconds. If the value is greater than 4 ms, the virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- The deviceLatency data counter measures the average amount of time, in milliseconds, to complete a SCSI command from the physical device. Depending on your hardware, a number greater than 15 ms indicates probable problems with the storage array. Move the active VMDK to a volume with more spindles or add disks to the LUN.
- The queueLatency data counter measures the average amount of time taken per SCSI command in the VMkernel queue. This value must always be zero. If not, the workload is too high and the array cannot process the data fast enough.

If the disk latency values are high, or if you notice other problems with disk I/O performance, consider taking the following actions.

Table 463: Disk I/O Performance Enhancement Advice

#	Resolution
1	Increase the virtual machine memory. It allows more operating system caching, which reduces I/O activity. Note: It might require you to increase the host memory. Increasing memory might reduce the need to store data because databases can utilize the system memory to cache data and avoid disk access. To verify that virtual machines have adequate memory, check swap statistics in the guest operating system. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
2	Defragment the file systems on all guests.
3	Disable antivirus on-demand scans on the VMDK and VMEM files.
4	Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. To increase throughput, consider array-side improvements.
5	Use Storage vMotion to migrate I/O-intensive virtual machines across multiple hosts.
6	Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
7	Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter. For more information, see *vSphere Storage*.
8	For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. It alleviates disk spindle contention during periods of high use.
9	On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
10	If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
11	For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
12	Use the most current host hardware.

Virtual Disk Requests (Number)

The Virtual Disk Requests chart displays virtual disk usage for the virtual machine.

After you click **Overview** on the **Performance** tab of the virtual machine, you can view this chart by selecting **Home** from the **View** drop-down menu. It is available at collection (display) levels 3 and 4.

Table 464: Data Counters

Chart Label	Description
Read Requests	Number of virtual disk read commands completed on each virtual disk on the virtual machine. The aggregate number of all virtual disk read commands is also displayed in the chart. • Counter: numberRead • Stats Type: Absolute

Chart Label	Description
	• Unit: Number • Rollup Type: Average • Collection Level: 2
Write Requests	Number of virtual disk write commands completed on each virtual disk on the virtual machine. The aggregate number of all virtual disk write commands is also displayed in the chart. • Counter: numberWrite • Stats Type: Absolute • Unit: Number • Rollup Type: Average • Collection Level: 2

Virtual Disk Rate (KBps)

The Virtual Disk Rate chart displays virtual disk usage rate for the virtual machine.

After you click **Overview** on the **Performance** tab of the virtual machine, you can view this chart by selecting **Home** from the **View** drop-down menu. It is available only at collection levels 3 and 4.

Table 465: Data Counters

Chart Label	Description
Read Requests	Number of virtual disk read commands completed on each virtual disk on the virtual machine. The aggregate number of all virtual disk read commands per second is also displayed in the chart. Read rate = blocksRead per second × blockSize • Counter: read • Stats Type: Rate • Unit: KiloBytes per second (KBps) • Rollup Type: Average • Collection Level: 3
Write Requests	Number of virtual disk write commands completed on each virtual disk on the virtual machine per second. The aggregate number of all virtual disk write commands per second is also displayed in the chart. Write rate = blocksWritten per second × blockSize • Counter: write • Stats Type: Rate • Unit: KiloBytes per second (KBps) • Rollup Type: Average • Collection Level: 3

Memory (%)

The Memory (%) chart monitors virtual machine memory usage.

This chart is located in the **Home** view of the virtual machine **Performance** tab.

Virtual Machine Counters

Note: Guest physical memory refers to the virtual hardware memory presented to a virtual machine for its guest operating system.

Table 466: Data Counters

Chart Label	Description
Usage	Amount of guest physical memory currently in use on the virtual machine. • Counter: usage • Stats Type: Absolute • Unit: Percentage (%) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 467: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory (MB)

The Memory (MB) chart displays virtual machine balloon memory.

This chart is located in the **Home** view of the virtual machine **Performance** tab.

Table 468: Data Counters

Chart Label	Description
Balloon	Amount of guest physical memory reclaimed from the virtual machine by the balloon driver. • Counter: vmmemctl • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 469: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory (MBps)

The Memory (MBps) chart displays virtual machine memory swap rates.

This chart is located in the **Home** view of the Virtual Machine **Performance** tab.

Table 470: Data Counters

Chart Label	Description
swapinRate	Average rate at which memory is swapped into the virtual machine. • Counter: swapinRate • Stats Type: Rate • Unit: MegaBytes per second (MBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
swapoutRate	Average rate at which memory is swapped out of the virtual machine. • Counter: swapoutRate • Stats Type: Rate • Unit: MegaBytes per second (MBps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If there is sufficient swap space, a high balloon value is not a performance issue. However, if the swapin and swapout values for the host are large, the host is probably lacking the memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. The host might require more memory resources. If it does not, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If memory usage is high or you notice degradation in performance, consider taking the following actions.

Table 471: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of a virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.

#	Resolution
6	Add physical memory to the host.

Memory (MB)

The Memory (MB) chart displays memory data counters for virtual machines.

This chart is located in the **Home** view of the virtual machine **Performance** tab. It appears only at collection levels 2, 3, and 4.

In the following descriptions, the guest physical memory refers to the virtual-hardware memory presented to a virtual machine for its guest operating system. Machine memory is actual physical RAM in the host. Note that not all counters are collected at collection level 1.

Table 472: Data Counters

Chart Label	Description
Active	Amount of guest physical memory in use by the virtual machine. Active memory is estimated by VMkernel statistical sampling and represents the actual amount of memory the virtual machine needs. The value is based on the current workload of the virtual machine. • Counter: active • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Balloon	Amount of guest physical memory reclaimed from the virtual machine by the balloon driver. • Counter: vmmemctl • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)
Balloon Target	Desired amount of virtual machine balloon memory. Balloon target memory is estimated by the VMkernel. If the balloon target amount is greater than the balloon amount, the VMkernel inflates the balloon amount, which reclaims more virtual machine memory. If the balloon target amount is less than the balloon amount, the VMkernel deflates the balloon, which allows the virtual machine to reallocate memory when needed. • Counter: vmmemctltarget • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Consumed	Amount of guest physical memory consumed by the virtual machine for guest memory. Consumed memory does not include overhead memory. It includes shared memory and memory that might be reserved, but not actually used. consumed memory = memory granted - memory saved due to memory sharing • Counter: consumed • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum)

Chart Label	Description
	• Collection Level: 1 (4)
Shared	Amount of guest physical memory available for sharing. Memory sharing occurs through transparent page sharing. • Counter: shared • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)
Swapped	The amount of guest physical memory swapped out to the disk by the VMkernel. This data counter measures VMkernel swapping and not to guest OS swapping. swapped = swapout – swapin **Note:** In some cases, vMotion can skew these values and cause a virtual machine to arrive on a host with some memory already swapped out. As a result, the swapped value can be greater than the swapout – swapin value. • Counter: swapped • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4)

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 473: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.

#	Resolution
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory Bandwidth (MBps)

The Memory Bandwidth chart for a displays the estimated DRAM Read bandwidth graph and estimated PMem Read Bandwith graphs for a virtual machine.

This chart is available in the **Memory** pane of the **View** dropdown menu of vSphere Client for a virtual machine at **Performance** > **Overview** tab. The **Memory** pane gives information about Memory Bandwidth in addition to the Memory Usage and Memory Reclamation information.

Note: If the host supports vMMR and is in memory mode, **Memory** option is listed in the **View** dropdown menu. In other cases, Memory option is not listed.

Table 474: Data Counters

Chart Label	Description
Estimated DRAM Read Bandwidth	Current read bandwidth of DRAM memory type. • Counter: bandwidth.read • Stats Type: Absolute • Unit: MegaBytes per second (MBps) • Rollup Type: Latest • Collection Level: 2 (4)
Estimated PMem Read Bandwidth	Current read bandwidth of PMem memory type. • Counter: bandwidth.read • Stats Type: Absolute • Unit: MegaBytes per second (MBps) • Rollup Type: Latest • Collection Level: 2 (4)

Network (Mbps)

The Network (Mbps) chart displays network bandwidth for the virtual machine.

This chart is located in the **Home** view of the Virtual Machine **Performance** tab.

Table 475: Virtual Machine Counters

Chart Label	Description
Usage	Average rate at which data is transmitted and received across all virtual NIC instances connected to the virtual machine. • Counter: usage • Stats Type: Rate

Chart Label	Description
	• Unit: Megabits per second (Mbps) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 1 (4)

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 476: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Network Rate (Mbps)

The Network Rate chart displays network usage for virtual machines.

This chart is located in the **Home** view of the Virtual Machine **Performance** tab. It appears only at collection levels 3 and 4.

Table 477: Data Counters

Chart Label	Description
Data Receive Rate	Rate at which data is received across each virtual NIC instance on the virtual machine. • Counter: received • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average • Collection Level: 2 (4)
Data Transmit Rate	Rate at which data is transmitted across each virtual NIC instance on the virtual machine. • Counter: transmitted • Stats Type: Rate • Unit: Megabits per second (Mbps) • Rollup Type: Average • Collection Level: 2 (4)

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 478: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.

#	Resolution
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Network Packets (Number)

The Network Packets monitors network bandwidth for virtual machines.

This chart is located in the **Home** view of the Virtual Machine **Performance** tab. It appears only at collection levels 3 and 4.

Table 479: Data Counters

Chart Label	Description
Packets Transmitted	Number of network packets transmitted across the top ten virtual NIC instances on the virtual machine. The chart also displays the aggregated value for each NIC. • Counter: packetTx • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3
Packets Received	Number of network packets received across the top ten virtual NIC instances on the virtual machine. The chart also displays the aggregated value for each NIC. • Counter: packetRx • Stats Type: Absolute • Unit: Number • Rollup Type: Summation • Collection Level: 3

Chart Analysis

Network performance depends on the application workload and network configuration. Dropped network packets indicate a bottleneck in the network. To determine whether packets are being dropped, use `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values.

If packets are being dropped, adjust the virtual machine shares. If packets are not being dropped, check the size of the network packets and the data receive and transfer rates. In general, the larger the network packets, the faster the

network speed. When the packet size is large, fewer packets are transferred, which reduces the amount of CPU required to process the data. When network packets are small, more packets are transferred but the network speed is slower because more CPU is required to process the data.

Note: In some instances, large packets might result in a high network latency. To check the network latency, use the VMware AppSpeed performance monitoring application or a third-party application.

If packets are not being dropped and the data receive rate is slow, the host is probably lacking the CPU resources required to handle the load. Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different vSwitches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.

If you experience network-related performance problems, also consider taking the following actions.

Table 480: Networking Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine.
2	If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
3	If virtual machines running on the same host communicate with each other, connect them to the same vSwitch to avoid transferring packets over the physical network.
4	Assign each physical NIC to a port group and a vSwitch.
5	Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
6	Ensure that the physical NIC capacity is large enough to handle the network traffic on that vSwitch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10 Gbps). Alternatively, consider moving some virtual machines to a vSwitch with a lighter load or to a new vSwitch.
7	If packets are being dropped at the vSwitch port, increase the virtual network driver ring buffers where applicable.
8	Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that NICs with 1 Gbps are not reset to 100 Mbps because they are connected to an older switch.
9	Verify that all NICs are running in full duplex mode. Hardware connectivity problems might result in a NIC resetting itself to a lower speed or half duplex mode.
10	Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TSO-Jumbo Frames are enabled where possible.

Space in GB

The Space in GB chart displays space utilization data counters for virtual machines.

This chart is located in the **Storage** view of the virtual machine **Performance** tab.

Table 481: Data Counters

Chart Label	Description
Allocated	Total amount of logical datastore space provisioned by an administrator for the virtual machine. It is the storage size up to which the virtual machine files on datastores can grow. This includes log files, VMX files, and other miscellaneous files. Allocated space is not always in use. • Counter: provisioned • Stats Type: Absolute

Chart Label	Description
	• Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1
Used	Amount of physical datastore space in use by the virtual machine files. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1
Not Shared	Amount of datastore space that belongs only to this virtual machine and is not shared with other virtual machines. Only unshared space is guaranteed to be reclaimed for the virtual machine if, for example, it is moved to a different datastore and then back again. The value is an aggregate of all unshared space for the virtual machine, across all datastores. • Counter: unshared • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space Utilization by Datastores

The Space Utilization by Datastores chart displays the amount of space used by a virtual machine on different datastores in the data center.

Note: This chart does not show historical statistics. It only shows the most recently available data, which may be up to 30 minutes late, depending on when the last statistics rollup occurred. In addition, statistics are not collected across all datastores at one time. They are collected asynchronously.

The Space Utilization by Datastores chart is located in the **Storage** view of the virtual machine **Performance** tab.

Table 482: Data Counters

Chart Label	Description
datastore_name	Amount of disk space in the datastore currently in use by the virtual machine. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Space Utilization By File Type

The Space Utilization by File Type chart displays the datastore usage by virtual machine files.

Note: This chart does not show historical statistics. It only shows the most recently available data, which may be up to 30 minutes late, depending on when the last statistics rollup occurred. In addition, statistics are not collected across all datastores at one time. They are collected asynchronously.

The Space Utilization by File Type chart is located in the **Storage** view of the virtual machine **Performance** tab.

Datastore counters

Table 483: Data Counters

File Type	Description
Virtual Disks	Amount of disk space used by virtual disk files. Virtual disk files store the contents of the virtual machine's hard disk drive, including information that you write to a virtual machine's hard disk - the operating system, program files, and data files. The files have the extension `.vmdk` and appear as a physical disk drive to a guest operating system. **Note:** Delta disks, which also have an extension `.vmdk`, are not included in this file type. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Swap Files	Amount of disk space used by swap files. Swap files back up the virtual machine's physical memory. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Snapshots	Amount of disk space used by virtual machine snapshot files. Snapshot files store information about virtual machine snapshots. They include snapshot state files and delta disk files. A snapshot state file stores the running state of the virtual machine at the time of the snapshot. It has the extension `.vmsn`. A delta disk file stores the updates made by the virtual machine to the virtual disks after a snapshot is taken. • Counter: used • Stats Type: Absolute • Unit: GigaBytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)

File Type	Description
Other VM Files	Amount of disk space used by all other virtual machine files, such as configuration files and log files. • Counter: used • Stats Type: Absolute • Unit: Gigabytes (GB) • Rollup Type: Latest • Collection Level: 1 (4)
Total Space	Amount of disk space used by the virtual machine. total space = virtual disk space + swap file space + snapshot space + other VM file space

Chart Analysis

The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks. If possible, you can provision more space to the datastore, or you can add disks to the datastore or use shared datastores.

If snapshot files are consuming high datastore space, consider consolidating them to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface. For information about consolidating the data center, see the vSphere documentation.

Fault Tolerance Performance Counters

The fault tolerance charts contain information about CPU and memory for fault tolerant virtual machines.

Note: The performance charts and help topics for fault tolerance are available only when you have vSphere Fault Tolerance enabled. If you select a link for a secondary virtual machine in the thumbnail section of the Resource Pools and Virtual Machines view of the cluster Performance tab, the navigation in the inventory updates to the primary virtual machine. This occurs because secondary machines are not displayed in the inventory.

CPU (MHz)

The CPU (MHz) chart displays virtual CPU usage for fault tolerant virtual machines.

This chart is located in the **Fault Tolerance** view of the virtual machine **Peformance** tab. It is available only at collection levels 3 and 4.

Table 484: Data Counters

Name	Description
Usage	The average amount of virtual CPU, per CPU instance, in use on the primary and secondary fault tolerant virtual machines. • Counter: usagemhz • Stats Type: Rate • Unit: Megahertz (MHz) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 3 (4)

Chart Analysis

A large discrepancy in CPU usage between the primary and secondary virtual machines might indicate performance problems. The CPU ready, system, and wait times of each virtual machine should be synchronized. A large discrepancy in these values might indicate performance problems. Consider taking the following actions.

Table 485: CPU Performance Enhancement Advice

#	Resolution
1	Verify that the primary and secondary hosts are in the same CPU model family and have similar CPU configurations. For best results, use CPUs with the same stepping level.
2	Verify that the CPU resource reservations set for both virtual machines are consistent within the cluster. VMware HA plans for a worst-case scenario by considering all powered on virtual machines in a cluster and finding the maximum memory and CPU reservations.
3	Verify that the network and datastore connections for both virtual machines are similar.
4	Turn off power management (also known as power-capping) in the BIOS. If power management is enabled, the secondary host might enter lower performance, power-saving modes. Such modes can leave the secondary virtual machine with insufficient CPU resources, potentially making it impossible for the secondary to complete all tasks completed on a primary in a timely fashion.
5	Turn off hyperthreading in the BIOS. If hyperthreading is enabled and the secondary virtual machine is sharing a CPU with another demanding virtual machine, the secondary virtual machine might run too slowly to complete all tasks completed on the primary in a timely fashion.

CPU System Time for vCPU (%)

The CPU System Time chart displays virtual CPU usage for fault tolerant virtual machines.

This chart is located in the **Fault Tolerance** view of the Virtual Machine **Peformance** tab. It is available only at collection levels 3 and 4.

Table 486: Data Counters

Chart Label	Description
System	Amount of time spent on system processes on each virtual CPU in the virtual machine. **Note:** This is the host view of the CPU usage, not the guest operating system view. • Counter: system • Stats Type: Delta • Unit: Percentage (%) • Rollup Type: Summation • Collection Level: 3

Chart Analysis

A large discrepancy in CPU usage between the primary and secondary virtual machines might indicate performance problems. The CPU ready, system, and wait times of each virtual machine should be synchronized. A large discrepancy in these values might indicate performance problems. Consider taking the following actions.

Table 487: CPU Performance Enhancement Advice

#	Resolution
1	Verify that the primary and secondary hosts are in the same CPU model family and have similar CPU configurations. For best results, use CPUs with the same stepping level.

#	Resolution
2	Verify that the CPU resource reservations set for both virtual machines are consistent within the cluster. VMware HA plans for a worst-case scenario by considering all powered on virtual machines in a cluster and finding the maximum memory and CPU reservations.
3	Verify that the network and datastore connections for both virtual machines are similar.
4	Turn off power management (also known as power-capping) in the BIOS. If power management is enabled, the secondary host might enter lower performance, power-saving modes. Such modes can leave the secondary virtual machine with insufficient CPU resources, potentially making it impossible for the secondary to complete all tasks completed on a primary in a timely fashion.
5	Turn off hyperthreading in the BIOS. If hyperthreading is enabled and the secondary virtual machine is sharing a CPU with another demanding virtual machine, the secondary virtual machine might run too slowly to complete all tasks completed on the primary in a timely fashion.

CPU Used Time for vCPU (%)

The CPU Used Time chart displays virtual CPU usage for fault tolerant virtual machines.

This chart is located in the **Fault Tolerance** view of the Virtual Machine **Peformance** tab. The chart is available only for collection levels 3 and 4.

Table 488: Data Counters

Chart Label	Description
used	Amount of used virtual CPU as a percentage of total available CPU on the primary and secondary virtual machines. A high value indicates excessive use of CPU resources. • Counter: used • Stats Type: Delta • Unit: Percentage (%) • Rollup Type: Summation • Collection Level: 1

Chart Analysis

A large discrepancy in CPU usage between the primary and secondary virtual machines might indicate performance problems. The CPU ready, system, and wait times of each virtual machine should be synchronized. A large discrepancy in these values might indicate performance problems. Consider taking the following actions.

Table 489: CPU Performance Enhancement Advice

#	Resolution
1	Verify that the primary and secondary hosts are in the same CPU model family and have similar CPU configurations. For best results, use CPUs with the same stepping level.
2	Verify that the CPU resource reservations set for both virtual machines are consistent within the cluster. VMware HA plans for a worst-case scenario by considering all powered on virtual machines in a cluster and finding the maximum memory and CPU reservations.
3	Verify that the network and datastore connections for both virtual machines are similar.

#	Resolution
4	Turn off power management (also known as power-capping) in the BIOS. If power management is enabled, the secondary host might enter lower performance, power-saving modes. Such modes can leave the secondary virtual machine with insufficient CPU resources, potentially making it impossible for the secondary to complete all tasks completed on a primary in a timely fashion.
5	Turn off hyperthreading in the BIOS. If hyperthreading is enabled and the secondary virtual machine is sharing a CPU with another demanding virtual machine, the secondary virtual machine might run too slowly to complete all tasks completed on the primary in a timely fashion.

Memory Active (MB)
The Memory Active chart displays active memory usage for fault tolerant virtual machines.

This chart is located in the **Fault Tolerance** view of the Virtual Machine **Peformance** tab. It is not available at collection level 1.

Table 490: Data Counters

Chart Label	Description
Active	Amount of guest physical memory in use by the fault tolerant virtual machine. Active memory is estimated by VMkernel statistical sampling and represents the actual amount of memory the virtual machine needs. Additional, unused memory may be swapped out or ballooned with no performance impact. • Counter: active • Stats Type: Absolute • Unit: Megabytes (MB) • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4) Make sure that the primary and secondary virtual machines have enough memory. If the secondary system is not provisioned well, it might slow down performance of the primary virtual machine or fail.

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If sufficient swap space is available, a high balloon value does not cause performance problems. However, if the swapin and swapout values for the host are large, the host is probably lacking the amount of memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. A free memory value of 6% or less indicates that the host cannot meet the memory requirements. This leads to memory reclamation, which might degrade performance. If the active memory size is the same as the granted memory size, demand for memory is greater than the memory resources available. If the active memory is consistently low, the memory size might be too large.

If the host has enough free memory, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If little free memory is available, or if you notice degradation in performance, consider taking the following actions.

Table 491: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Memory Swapout (MB)
The Memory Swapout chart displays the swapout memory usage for fault tolerant virtual machines.

This chart is located in the **Fault Tolerance** view of the Virtual Machine **Peformance** tab. It is not available at collection level 1.

Table 492: Data Counters

Chart Label	Description
Swapout	Amount of machine memory written to the VMkernel swap file. • Counter: swapout • Stats Type: Absolute • Unit: MegaBytes • Rollup Type: Average (Minimum/Maximum) • Collection Level: 2 (4) Make sure that the primary and secondary virtual machines have enough memory and that the swapout value is not high. If the secondary system is not provisioned well, it might slow down performance of the primary virtual machine or fail.

Chart Analysis

A virtual machine's memory size must be slightly larger than the average guest memory usage. This enables the host to accommodate workload spikes without swapping memory among guests. Increasing the virtual machine memory size results in more overhead memory usage.

If there is sufficient swap space, a high balloon value is not a performance issue. However, if the swapin and swapout values for the host are large, the host is probably lacking the memory required to meet the demand.

If a virtual machine has high ballooning or swapping, check the amount of free physical memory on the host. The host might require more memory resources. If it does not, check the resource shares, reservation, and limit of the virtual machines and resource pools on the host. Verify that the host settings are adequate and not lower than those set for the virtual machine.

If memory usage is high or you notice degradation in performance, consider taking the following actions.

Table 493: Memory Performance Enhancement Advice

#	Resolution
1	Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
2	Verify that the balloon driver is enabled. The VMkernel regularly reclaims unused virtual machine memory by ballooning and swapping. Generally, this does not impact virtual machine performance.
3	Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
4	If the memory reservation of a virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
5	Migrate one or more virtual machines to a host in a DRS cluster.
6	Add physical memory to the host.

Working with Advanced and Custom Charts

Use advanced charts, or create your own custom charts, to see more performance data. Advanced charts can be useful when you are aware of a problem but need more statistical data to pinpoint the source of the trouble.

Advanced charts include the following features:

- More information. Hover over a data point in a chart and details about that specific data point are displayed.
- Customizable charts. Change chart settings. To create your own charts, save custom settings.
- Export to spreadsheet.
- Save to image file or spreadsheet.

View Advanced Performance Charts in the vSphere Client

Advanced charts support data counters that are not supported in other performance charts.

1. Navigate to an inventory object in the vSphere Client.
2. Click the **Monitor** tab, and click **Performance**.
3. Click **Advanced**.
4. Optional: To view a different chart, select an option from the **View** list.

   The amount of historical data displayed in a chart depends on the collection interval and statistics level set for vCenter Server.
5. Optional: To view the selected performance chart in a popup window, click the **Popup Chart** icon ( ). The chart opens in a new browser window enabling you to navigate within the vSphere Client while keeping the performance chart open in a separate window. You can learn more about this feature in this video.

Change Advanced Chart Settings

You can customize a performance chart by specifying the objects to monitor, the counters to include, the time range, and chart type. You can customize preconfigured chart views and create chart views.

1. Select an inventory object in the vSphere Client.
2. Click the **Monitor** tab, and click **Performance**.
3. Click **Advanced**.
4. Click **Chart Options**.
5. In Chart Metrics, select a metric group for the chart.
6. Select a time range for the metric group.

   Time range options are not active unless you select **Custom interval** in the **Timespan** menu.

   If you choose **Custom interval**, do one of the following.

   - Select **Last** and set the number of hours, days, weeks, or months for the amount of time to monitor the object.
   - Select **From** and select the beginning and end dates.

   You can also customize the time range options by customizing the statistics collection interval setting.
7. In Target Objects, select the inventory objects to display in the chart.

   You can also specify the objects using the **All** or **None** buttons.
8. Select the chart type.

   When selecting the stacked graph option, consider the following.

   - You can select only one item from the list of measurements.
   - Per-virtual-machine stacked graphs are available only for hosts.
   - To display information about the counter's function and whether the selected metric can be stacked for per-virtual-machine graphs, click a counter description name.
9. In Counters, select the data counters to display in the chart.

   You can also specify counters using the **All** or **None** buttons. The **All** button is inactive when there are more than two different counter units for the corresponding metric group.
10. Click **OK**.

Create a Custom Advanced Chart

You can create your own charts by saving customized chart settings. New charts are added to the **View** menu and will appear there only when charts for the selected object are being displayed.

1. Select an inventory object in the vSphere Client.
2. Click the **Monitor** tab, click **Performance**, and navigate to the Chart Options dialog of a chart.
3. Customize chart settings.
4. Click **Save Options As...**.
5. Enter a name for your settings.
6. Click **OK**.

The chart settings are saved and an entry for your chart is added to the **View** menu.

Related Links

Change Advanced Chart Settings on page 3236

You can customize a performance chart by specifying the objects to monitor, the counters to include, the time range, and chart type. You can customize preconfigured chart views and create chart views.

Delete a Custom Advanced Chart View

You can delete custom chart views from the vSphere Client.

1. Select an inventory object in the vSphere Client.
2. Click the **Monitor** tab, and click **Performance**.
3. Click **Advanced**.
4. Click **Chart Options**.
5. Select a chart and click **Delete Options**.
6. Click **OK** to confirm deletion.
   The chart is deleted, and it is removed from the **View** menu.

Save Chart Data to a File

You can save data from the advanced performance charts to a file in various graphic formats or in comma-separated values (CSV) format.

1. In the vSphere Client, select an inventory object.
2. Click the **Monitor** tab, and click **Performance**.
3. Click **Advanced**.
4. Click the **Export** icon ( ).
5. Select a file type.

Option	Description
To PNG	Exports a bitmap image in the PNG format.
To JPEG	Exports a bitmap image in the JPEG format.
To CSV	Exports plain-text data in the CSV format.
To SVG	Exports a vector image in the SVG format. **Note:** This option is available only in the vSphere Client.

6. Enter a name and location for the file.
7. Click **Save**.

The file is saved to the location and format you specified.

Troubleshoot and Enhance Performance

This section presents tips for identifying and solving performance problems.

The suggestions in this section are not meant to be a comprehensive guide to diagnosing and troubleshooting problems in the virtual environment. It is meant to provide information about some common problems that can be solved without contacting VMware Technical Support.

Solutions for Consistently High CPU Usage

Temporary spikes in CPU usage are not necessarily a concern, but consistently high CPU usage might indicate a problem. You can use the CPU performance charts to monitor CPU usage for hosts, clusters, resource pools, virtual machines, and vApps.

- Host CPU usage constantly is high. A high CPU usage value can lead to increased ready time and processor queuing of the virtual machines on the host.
- Virtual machine CPU usage is above 90% and the CPU ready value is above 20%. Application performance is impacted.
- The host probably is lacking the CPU resources required to meet the demand.
- There might be too many virtual CPUs relative to the number of physical processor cores.
- There might be an IO storage or networking operation that places the CPU in a wait state.
- The Guest OS generates too much load for the CPU.
- Verify that VMware Tools is installed on every virtual machine on the host.
- Compare the CPU usage value of a virtual machine with the CPU usage of other virtual machines on the host or in the resource pool. The stacked bar chart on the host's **Virtual Machine** view shows the CPU usage for all virtual machines on the host.
- Determine whether the high ready time for the virtual machine resulted from its CPU usage time reaching the CPU limit setting. If so, increase the CPU limit on the virtual machine.
- Increase the CPU shares to give the virtual machine more opportunities to run. The total ready time on the host might remain at the same level if the host system is constrained by CPU. If the host ready time does not decrease, set the CPU reservations for high-priority virtual machines to guarantee that they receive the required CPU cycles.
- Increase the amount of memory allocated to the virtual machine. This can potentially decrease disk and/or network activity for applications that cache. This might lower disk I/O and/or network traffic, which could in turn reduce CPU utilization. Virtual machines with smaller resource allocations generally accumulate more CPU ready time.
- Reduce the number of virtual CPUs on a virtual machine to only the number required to execute the workload. For example, a single-threaded application on a four-way virtual machine only benefits from a single vCPU. But the ESXi's maintenance of the three idle vCPUs takes CPU cycles that could be used for other work.
- If the host is not already in a DRS cluster, add it to one. If the host is in a DRS cluster, increase the number of hosts and migrate one or more virtual machines onto the new host.
- Upgrade the physical CPUs on the host if necessary.
- Use the newest version of hypervisor software, and enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.

Solutions for Memory Performance Problems

Host machine memory is the hardware backing for guest virtual memory and guest physical memory. For best performance, the host machine memory should be at least slightly larger than the combined active memory of the virtual machines on the host. A virtual machine's memory size should be slightly larger than the average guest memory usage. Increasing the virtual machine memory size results in more overhead memory usage.

- Memory usage is constantly high (94% or greater) or constantly low (24% or less).
- Free memory consistently is 6% or less and swapping frequently occurs.
- The host probably is lacking the memory resources required to meet the combined active memory size of all the running VMs.
- Host machine memory resources are not enough to meet the demand, which leads to memory reclamation (like swapping) and degraded performance.

- Verify that VMware Tools is installed on each virtual machine. The balloon driver is installed with VMware Tools and is critical to performance.
- Verify that the balloon driver is enabled. The VMkernel regularly attempts to reclaim the unused virtual machine memory by ballooning and, if necessary, swapping. Generally, this does not impact virtual machine performance.
- Reduce the memory space on the virtual machine, and correct the cache size if it is too large. This frees up memory for other virtual machines.
- If the memory reservation of the virtual machine is set to a value much higher than its active memory, decrease the reservation setting so that the VMkernel can reclaim the idle memory for other virtual machines on the host.
- Migrate one or more virtual machines to a host in a DRS cluster.
- Add physical memory to the host.

Solutions for Storage Performance Problems

Datastores represent storage locations for virtual machine files. A storage location can be a VMFS volume, a directory on Network Attached Storage, or a local file system path. Datastores are platform-independent and host-independent.

- Snapshot files are consuming a lot of datastore space.
- The datastore is at full capacity when the used space is equal to the capacity. Allocated space can be larger than datastore capacity, for example, when you have snapshots and thin-provisioned disks.
- Consider consolidating snapshots to the virtual disk when they are no longer needed. Consolidating the snapshots deletes the redo log files and removes the snapshots from the vSphere Client user interface.
- You can provision more space to the datastore if possible, or you can add disks to the datastore or use shared datastores.

Solutions for Disk Performance Problems

Use the disk charts to monitor average disk loads and to determine trends in disk usage. For example, you might notice a performance degradation with applications that frequently read from and write to the hard disk. If you see a spike in the number of disk read/write requests, check if any such applications were running then.

- The value for the kernelLatency data counter is greater than 4 ms.
- The value for the deviceLatency data counter is greater than 15 ms indicates that there are probably problems with the storage array.
- The queueLatency data counter measures above zero.
- Spikes in latency.
- Unusual increases in read/write requests.
- The virtual machines on the host are trying to send more throughput to the storage system than the configuration supports.
- The storage array probably is experiencing internal problems.
- The workload is too high and the array cannot process the data fast enough.

- The virtual machines on the host are trying to send more throughput to the storage system than the configuration supports. Check the CPU usage, and increase the queue depth.
- Move the active VMDK to a volume with more spindles or add disks to the LUN.
- Increase the virtual machine memory. Doing so should allow for more operating system caching, which can reduce I/O activity. Note: It may require you to increase the host memory. Increasing memory might reduce the need to store data because some workloads can utilize system memory to cache data and avoid disk access.
- Check swap statistics in the guest operating system to verify that virtual machines have adequate memory. Increase the guest memory, but not to an extent that leads to excessive host memory swapping. Install VMware Tools so that memory ballooning can occur.
- Defragment the file systems on all guests.
- If appropriate for your environment, disable antivirus on-demand scans on the VMDK and VMEM files.
- Use the vendor's array tools to determine the array performance statistics. When too many servers simultaneously access common elements on an array, the disks might have trouble keeping up. Consider array-side improvements to increase throughput.
- Use Storage vMotion to distribute I/O-intensive virtual machines across multiple hosts.
- Balance the disk load across all physical resources available. Spread heavily used storage across LUNs that are accessed by different adapters. Use separate queues for each adapter to improve disk efficiency.
- Configure the HBAs and RAID controllers for optimal use. Verify that the queue depths and cache settings on the RAID controllers are adequate. If not, increase the number of outstanding disk requests for the virtual machine by adjusting the `Disk.SchedNumReqOutstanding` parameter.
- For resource-intensive virtual machines, separate the virtual machine's physical disk drive from the drive with the system page file. This alleviates disk spindle contention during periods of high use.
- On systems with sizable RAM, disable memory trimming by adding the line `MemTrimRate=0` to the virtual machine's VMX file.
- If the combined disk I/O is higher than a single HBA capacity, use multipathing or multiple links.
- For ESXi hosts, create virtual disks as preallocated. When you create a virtual disk for a guest operating system, select **Allocate all disk space now**. The performance degradation associated with reassigning additional disk space does not occur, and the disk is less likely to become fragmented.
- Use the most current hypervisor software.

Solutions for Poor Network Performance

Network performance is dependent on application workload and network configuration. Dropped network packets indicate a bottleneck in the network. Slow network performance can be a sign of load-balancing problems.

Network problems can manifest in many ways:

- Packets are being dropped.
- Network latency is high.
- Data transfer rate is low.

Network problems can have several causes:

- Virtual machine network resource shares are too few.
- Network packet size is too large, which results in high network latency. Use the VMware AppSpeed performance monitoring application or a third-party application to check network latency.
- Network packet size is too small, which increases the demand for the CPU resources needed for processing each packet. Host CPU, or possibly virtual machine CPU, resources are not enough to handle the load.

- Determine whether packets are being dropped by using `esxtop` or the advanced performance charts to examine the `droppedTx` and `droppedRx` network counter values. Verify that VMware Tools is installed on each virtual machine.
- Check the number of virtual machines assigned to each physical NIC. If necessary, perform load balancing by moving virtual machines to different virtual switches or by adding more NICs to the host. You can also move virtual machines to another host or increase the host CPU or virtual machine CPU.
- If possible, use vmxnet3 NIC drivers, which are available with VMware Tools. They are optimized for high performance.
- If virtual machines running on the same host communicate with each other, connect them to the same virtual switch to avoid the cost of transferring packets over the physical network.
- Assign each physical NIC to a port group and a virtual switch.
- Use separate physical NICs to handle the different traffic streams, such as network packets generated by virtual machines, iSCSI protocols, vMotion tasks.
- Ensure that the physical NIC capacity is large enough to handle the network traffic on that virtual switch. If the capacity is not enough, consider using a high-bandwidth physical NIC (10Gbps) or moving some virtual machines to a virtual switch with a lighter load or to a new virtual switch.
- If packets are being dropped at the virtual switch port, increase the virtual network driver ring buffers where applicable.
- Verify that the reported speed and duplex settings for the physical NIC match the hardware expectations and that the hardware is configured to run at its maximum capability. For example, verify that 1Gbps NICs are not reset to 100Mbps because they are connected to an older switch.
- Verify that all NICs are running in full duplex mode. Hardware connectivity issues might result in a NIC resetting itself to a lower speed or half duplex mode.
- Use vNICs that are TCP Segmentation Offload (TSO)-capable, and verify that TCP Segmentation Offload-Jumbo Frames are enabled where possible.

Empty Performance Charts

No graphics or data are displayed in performance charts.

When data is missing for a performance chart, the chart appears empty and you see the message `No data available`.

The causes for missing data in performance charts that are described herein are based on the assumption that the default roll-up configuration for the vCenter Server system has not changed. The causes include but are not limited to the following scenarios:

- Metrics introduced in ESXi 5.0 are not available for hosts running earlier versions.
- Data is deleted when you remove or add objects to vCenter Server.
- Performance charts data for inventory objects that were moved to a new site by VMware vCenter Site Recovery Manager is deleted from the old site and not copied to the new site.
- Performance charts data is deleted when you use VMware vMotion across vCenter Server instances.
- Real-time statistics are not available for disconnected hosts or powered off virtual machines.
- Real-time statistics are collected on hosts and aggregated every 5 minutes. After six data points are collected for approximately 30 minutes, they are rolled up to the vCenter Server database to create the 1-Day statistic. 1-Day statistics might not be available for 30 minutes after the current time, depending on when the sample period began.
- The 1-Day statistics are rolled up to create one data point every 30 minutes. If a delay occurs in the roll-up operation, the 1-Week statistics might not be available for 1 hour after the current time. It takes 30 minutes for the 1-Week collection interval, plus 30 minutes for the 1-Day collection interval.
- The 1-Week statistics are rolled up to create one data point every two hours. If a delay occurs in the roll-up operations, the 1-Month statistics might not be available for 3 hours. It takes 2 hours for the 1-Month collection interval, plus 1 hour for the 1-Week collection interval.
- The 1-Month statistics are rolled up to create one data point every day. If a delay occurs in the roll-up operations, the statistics might not be available for 1-day and 3 hours. It takes one day for the past year collection interval, plus 3 hours for the past month collection interval. During this time, the charts are empty.

- There is no solution available.

Solutions for Performance Issues With Memory Mode

Intel provides an Intel Optane Persistent Memory Mode (PMem), in which the hardware hides the DRAM as cache and exposes PMem as the system memory. Although PMem is cheaper than DRAM, it has higher access latency which could lead to performance degradation issues.

Performance degradation issues while using PMem in Memory Mode:

- If the active memory is higher than some percentage of the available DRAM memory, the VM performance could degrade as memory accesses may have to go to PMem.
- Any two random VMs can have higher level of page collision due to hardware implementation resulting in degraded VM performance even if the available DRAM memory is fully utilized.

vSphere performs real-time monitoring using vSphere Memory Monitoring and Remediation (vMMR). vMMR collects both Host level and VM level memory statistics like DRAM/PMem bandwidth, latency, miss rate which provides additional insights. This is helpful in analyzing if the host is experiencing issues due to running in Memory Mode and if there is a need to re-distribute workload. If the analysis indicates that some workloads are having performance degradation due to running on systems configured in Memory mode, the VMs can be migrated from the current host to other hosts to balance the load.

- Two preconfigured default alarms have been added based on the newly collected statistics. One at the host level (Host Memory Mode High Active DRAM Usage) and another at the VM level (Virtual Machine High PMem Bandwidth Usage). If the alarm condition is met, an event will be published to trigger the corresponding alarm. If alarm is triggered, then it is indicative that there may be some issue with Memory Mode on this system. You can further analyze, if it is a real problem by using Performance charts.
- You can also create custom alarms based on new performance metrics at cluster/host or VM level. For example, you can create an alarm if the PMem bandwidth is observed to be higher than some value. vMMR alarms only work on systems with Memory Mode. For more information on how to create a custom alarm, see Create or Edit Alarms section.
- If the host is experiencing a performance issue, then it can be narrowed down to CPU, Memory, Disk, or Network issue by looking at the existing performance charts.
  In vSphere Client, a new **Memory** pane is added under Performance tab for both Host and VM. The host level performance chart displays read/write bandwidth, missrate for the different memory types (DRAM, PMem). The VM Level performance chart displays DRAM and PMem read bandwidth of the VM. These performance charts help customers to analyze the statistics and determine if their application workload is regressed due to Memory Mode. For example, if significant higher PMem bandwidth is observed, it is indicative of issues originating due to Memory Mode and can be investigated further.
- You can also plot custom based performance charts at host and VM level by using **Advanced** option and plotting some of Memory Mode related metrices.
- From the VMs tab of an ESXi host, you can view a list containing performance information about all virtual machines that reside on the host. To display information about the Memory Mode impact on a virtual machine, click the view columns ( ) icon and select the newly added Active Memory, DRAM Read Bandwidth, and PMem Read Bandwidth metrices. This is helpful in identifying the most impacted VMs.

For more information on vMMR, see *vSphere Memory Monitoring and Remediation* document.

Monitoring Guest Operating System Performance

This section describes how to install and view VMware-specific performance data for virtual machines that run Microsoft Windows operating systems. VMware provides performance counters that enable you to view data on many aspects of guest operating system performance for the Microsoft Windows Perfmon utility.

Some virtualization processes dynamically allocate available resources depending on the status, or utilization rates, of virtual machines in the environment. It can make obtaining accurate information about the resource utilization (CPU utilization, in particular) of individual virtual machines, or applications running within virtual machines, difficult. VMware now provides virtual machine-specific performance counter libraries for the Windows Perfmon utility. It enables application administrators to access accurate virtual machine resource utilization statistics from within the Windows Perfmon utility.

You can take advantage of virtualized CPU performance counters to use performance tuning tools inside the guest operating system. See the *vSphere Virtual Machine Administration* documentation.

Enable Statistics Collection for Guest Operating System Performance Analysis

VMware-specific performance objects are loaded into Microsoft Windows Perfmon and enabled when VMware Tools is installed.

To display a performance chart for any performance object, you must add counters. See View Performance Statistics for Windows Guest Operating Systems

View Performance Statistics for Windows Guest Operating Systems

You can display VMware specific statistics in the Microsoft Windows Perfmon utility.

Verify that a virtual machine with a Microsoft Windows operating system and VMware Tools is installed.

1. Open a console to the virtual machine and log in.
2. Select **Start > Run**.
3. Enter **Perfmon** and press **Enter**.
4. In the Performance dialog box, click **Add** .
5. In the Add Counters dialog box, select **Use local computer counters**.
6. Select a virtual machine performance object.
   Virtual machine performance object names begin with **VM**.
7. Select the counters that you want to display for that object.
8. If the performance object has multiple instances, select the instances you want to display.
9. Click **Add**.
   The Performance dialog box displays data for the selected performance object.
10. Click **Close** to close the Add Counter dialog box and return to the Performance dialog box.

Monitoring Host Health Status

You can use the vSphere Client to monitor the state of host hardware components, such as CPU processors, memory, fans, and other components.

The host health monitoring tool allows you to monitor the health of a variety of host hardware components including:

- CPU processors
- Memory
- Fans
- Temperature
- Voltage
- Power
- Network
- Battery

- Storage
- Cable/Interconnect
- Software components
- Watchdog
- PCI devices
- Other

The host health monitoring tool presents data gathered using Systems Management Architecture for Server Hardware (SMASH) profiles. The information displayed depends on the sensors available on your server hardware. SMASH is an industry standard specification providing protocols for managing a variety of systems in the data center. For more information, see http://www.dmtf.org/standards/smash.

You can monitor host health status by connecting the vSphere Client to a vCenter Server system. You can also set alarms to trigger when the host health status changes.

Note: The interpretation of hardware monitoring information is specific for each hardware vendor. Your hardware vendor can help you understand the results of the host hardware components monitoring.

Monitor Hardware Health Status in the vSphere Client

You can monitor the health status of host hardware in the vSphere Client

1. Select a host in the vSphere Client .
2. Click the **Monitor** tab, and click **Hardware Health**.
3. Select the type of information to view.

Option	Description
Sensors	Displays all sensors arranged in a tree view. If the status is blank, the health monitoring service cannot determine the status of the component.
Storage Sensors	Displays the storage sensors.
Alerts and Warnings	Displays alerts and warnings.
System Event Log	Displays the system event log.

Monitoring and Diagnostics of vSphere Health

Skyline Health for vSphere enables you to identify and resolve potential issues before they have an impact to your environment. vSphere telemetry data is collected from data-centers globally. This data is further used to analyze pre-conditions in your vSphere environment related to stability and incorrect configurations. These issues are reported under Skyline Health for vSphere and resolution recommendations are provided. It enables VMware to enhance the issue detection without updating the vSphere installation. You can check the health of vSphere Host and vCenter Server.

VMware Skyline Health Diagnostics tool is a self-service diagnostics platform. This tool helps to detect issues in the vSphere and vSAN product line and provides recommendations in the form of a Knowledge Base article or remediation procedures to address the identified issues. vSphere administrators can use this tool to troubleshoot issues before contacting VMware Global Support Service.

Check health of the system using Skyline Health for vSphere

You can use the Skyline Health checks for vSphere to monitor the health of the system. You can run health checks and send the data to VMware for advanced analysis.

- You must participate in the Customer Experience Improvement Program to use online health checks.

- To perform the online health checks, vCenter Server must be able to communicate over the Internet.
  Note: If Customer Improvement Experience Program (CEIP) is not enabled, the Internet connectivity check is unavailable.

1. Navigate to vCenter Server or select a host in the vSphere Client navigator.
2. Click the **Monitor** tab, and click **Skyline Health**.
3. Expand **Online Health Connectivity** category and select the type of information to view.

Option	Description
Customer experience improvement program (CEIP)	The CEIP check verifies whether the program is enabled for your vCenter Server. If it is not, click the button next to the health check, navigate to the CEIP page, and enroll in the program. To enable CEIP, click **Configure CEIP**
Online health connectivity	The Internet connectivity check verifies that vCenter Server can communicate with *vmware.com* over the HTTPS/443 interface. If communication is successful, this check passes. If communication fails, the check indicates that the Internet connectivity is not available.
Number of Online health checks performed successfully	This provide information on number of online health checks performed successfully.
Advisor	The Skyline Advisor, included with your Production or Premier Support contract, enhances your proactive support experience with additional features and functionality, including automatic support log bundle transfer with Log Assist.
Audit CEIP Collected Data	When you choose to participate in CEIP, VMware collects technical information about your use of the products and services in CEIP reports on a regular basis. This information does not personally identify you. The latest collected data can be found on the vCenter Server.

4. Expand the following categories to view the related health warnings:
   - **Compute Health Checks**
   - **Network Health Checks**
   - **Security Health Checks**
   - **Self support Diagnostics**
   - **Storage Health Checks**
   - **General Health Checks**
5. Click the **RETEST** button to run the health checks and update the results immediately.
   You can click the **Ask VMware** button to open a knowledge base article that describes the health check and provides information about how to resolve the issue.

Analyse issues using VMware Skyline Health Diagnostics tool

VMware Skyline Health Diagnostics is a self-service diagnostics platform. This tool helps to detect issues in the vSphere and vSAN product line and provides solutions for them.

VMware Skyline Health Diagnostics tool uses the product log files to identify issues and provides recommendations in the form of a Knowledge Base article or procedure to remediate issues. vSphere administrators can use this tool to

troubleshoot issues before contacting VMware Global Support Service. For detailed information about this diagnostics tool, see VMware Skyline Health Diagnostics document.

1. Select a host instance in the vSphere Client.
2. Click the **Monitor** tab, and click **Skyline Health**.
3. From the **Self support Diagnostics** dropdown, click **VMware Skyline Health Diagnostics**.

Monitoring Events, Alarms, and Automated Actions

vSphere includes a user-configurable events and alarms subsystem. This subsystem tracks events happening throughout vSphere and stores the data in log files and the vCenter Server database. This subsystem also enables you to specify the conditions under which alarms are triggered. Alarms can change state from mild warnings to more serious alerts as system conditions change, and can trigger automated alarm actions. This functionality is useful when you want to be informed, or take immediate action, when certain events or conditions occur for a specific inventory object, or group of objects.

Events

Events are records of user actions or system actions that occur on objects in vCenter Server or on a host. Actions that might be recorded as events include, but are not limited to, the following examples:

- A license key expires
- A virtual machine is powered on
- A user logs in to a virtual machine
- A host connection is lost

Event data includes details about the event such as who generated it, when it occurred, and what type of event it is.

The types of events are:

Table 494: Event Types

Event Type	Description
Error	Indicates that a fatal problem has occurred in the system and terminates the process or operation.
Warning	Indicates that there is a potential risk to the system which needs to be fixed. This event does not terminate the process or operation.
Information	Describes that the user or system operation is completed successfully.
Audit	Provides important audit log data which is crucial for the security framework. The audit log data includes information about what is the action, who did it, when it occurred, and the IP address of the user. You can learn more about this in the *vSphere Security* guide.

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an inventory object. An alarm definition consists of the following elements in the vSphere Client:

- Name and description - Provides an identifying label and description.

- Targets - Defines the type of object that is monitored.
- Alarm Rules - Defines the event, condition, or state that triggers the alarm and defines the notification severity. It also defines operations that occur in response to triggered alarms.
- Last modified - The last modified date and time of the defined alarm.

Alarms have the following severity levels:

- Normal – green
- Warning – yellow
- Alert – red

Alarm definitions are associated with the object selected in the inventory. An alarm monitors the type of inventory objects specified in its definition.

For example, you might want to monitor the CPU usage of all virtual machines in a specific host cluster. You can select the cluster in the inventory, and add a virtual machine alarm to it. When enabled, that alarm monitors all virtual machines running in the cluster and triggers when any one of them meets the criteria defined in the alarm. To monitor a specific virtual machine in the cluster, but not others, select that virtual machine in the inventory and add an alarm to it. To apply the same alarms to a group of objects, if they do not have common parent (datacenter, cluster or host), place those objects in a folder and define the alarm on the folder.

Note: You can modify alarms only from the object in which the alarm is defined. For example, if you defined an alarm in a cluster to monitor virtual machines, you can only modify that alarm through the cluster. You cannot change the alarm at the individual virtual machine level. However, you can disable or re-enable an alarm on a specific leaf inventory entity. For example, if a virtual machine related alarm is enabled on a vCenter level it can be disabled on a specific virtual machine and thus the alarm status for the specific entity will not be calculated and alarm state will be reset to gray.

Alarm Actions

Alarm actions are operations that occur in response to the trigger. For example, you can have an email notification sent to one or more administrators when an alarm is triggered.

Note: Default alarms are not preconfigured with actions. You must manually set what action occurs when the triggering event, condition, or state occurs.

View Events in vSphere Client

You can view events associated with a single object or view all vSphere events. The events list for a selected inventory object includes events associated with child objects. vSphere keeps information about tasks and events for a specified time period. You can configure this time period. By default, this period is set to 30 days.

1. Select an inventory object in the vSphere Client.
2. Click the **Monitor** tab, and click **Events**.
3. Click the expand row icon in each row to view the details for the corresponding event. You can expand multiple rows simultaneously.
4. Optional: Click the new tab icon at the top right corner of the datagrid to open the events view in a new tab.

   When you open the new tab from **Entity** > **Monitor** > **Events** menu, the name of the entity is displayed next to the title in the new tab. Click **REFRESH** at the top right of the datagrid in the new tab to refresh the events in the current page.
5. Optional: The `Triggering Event` column in the **Alarms** tab of bottom panel adjacent to `Recent Tasks` tab displays `"object-name: alarm-name"`. You can click on the hyperlink text to navigate to a particular object's events view. All the event details related to the selected alarm gets displayed. You can click on the **BACK TO ALL EVENTS** button to return to the default event-list view.

   For the alarms, that do not have any underneath event, a plain text is used.

Export Events in vSphere Client

You can export events using the vSphere client into a `.csv` file.

You can export selected or all events using the export option provided by vSphere Client.

1. Select an inventory object in the vSphere Client.
2. Click the **Monitor** tab, and click **Events**.
3. Select one or more events from the event list and click **Export** option available at the bottom left of the datagrid.

   Note: If you do not select any event and click **Export**, by default, all the rows in the current page of the datagrid are exported into a `.csv` file.

View System Event Log

vSphere records events in the vCenter Server database. System log entries include such information as who generated the event, when the event was created, and the type of event.

- Required privilege: **Global** > **Diagnostics**

1. Select a host in the vSphere Client navigator.
2. Click **Monitor** tab, and click **Hardware Health**.
3. Click **SYSTEM EVENT LOG**.

Export System Event Log Data

You can export all or part of the system event log data stored in the vCenter Server database.

Required Role: **Read-only**

1. Select a host in the vSphere Client.
2. Click the **Monitor** tab, and click **Hardware Health**.
3. Click the **SYSTEM EVENT LOG** option.
4. Click **EXPORT**.

Consolidate Identical Events

The event burst filter monitors the incoming stream of events for identical events over a short time. To optimize the storage size of events, events that occur repeatedly are consolidated into a single event before storing them in the database or the remote syslog server.

Event bursts can be seen in various scenarios which include,

- An existing hardware failure.
- An automated solution which logs-in and logs-out of vCenter Server often.

The events burst filter is enabled by default. It consolidates all types of events except those events on the allow list. An event burst is defined as more than one identical event per second. Two events are identical if,

- The events are of the same type.
- The events are on the same inventory object.
- The events are issued by the same user.

Note: The remaining event-specific data is not used to determine if two events are identical.

An event burst is detected after seeing 30 identical events for less than 30 seconds. These 30 events are stored in the VC database or the remote syslog server. Consolidation of the bursting events starts from the 31st event. The bursting events do not go into the database, but the consolidated event gets stored in the database.

In cases of bursting events, the burst filter affects only the events that go to the database and remote syslog stream. Alarms triggered by bursting events and `EventHistoryCollector` objects are not affected.

- `com.vmware.vc.EventBurstStartedEvent` - the start of an event burst.
- `com.vmware.vc.EventBurstEndedEvent` - the end of an event burst.
- `com.vmware.vc.AllEventBurstsEndedEvent` - the end of all the events bursts.
- `com.vmware.vc.EventBurstCompressedEvent` - the consolidated event after the event burst.

Each of this event contains,

- `eventType` - the event type of the bursting event.
- `objectId` - the entity of the bursting event.
- `userName` - the user name of the bursting event.

Also the compressed event contains,

- `count` - the number of identical events since the start of an event burst. The count starts from the 31st event.
- `burstStartTime` - Time of the 31st event of an event burst.
  Note: The timestamps of the burst filter events are not related to the bursting events.

Configure Events Burst Filter

You can configure the basic and advanced settings for the events burst filter in the advanced vCenter Server settings.

Burst filter can be in the following configurations.

- **Enabled**: If `compressToDb` or `compressToSyslog` are enabled, then the burst filter detects bursts, posts events for them, and consolidates events before storing them in the database or sending them to the remote syslog server.
- **Disabled**: The burst filter does not detect bursts, does not post events for them, and does not consolidate events before storing them in the database or sending them to the remote syslog server. If both `compressToDb` and `compressToSyslog` are disabled, then the burst filter detects bursts and posts events for them but does not consolidate events.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. **Advanced Settings**
4. Click **Edit**.
5. Click on the filter text box present in the **Name** column of the table header. Type `vpxd.event`, and press Enter.
6. For the basic setting,
   a) Enable or disable the vpxd.event.burstFilter.compressToDb option.
      This option enables you to compress the bursting of events in the database. The default value for the setting is enabled.
   b) Enable or disable the vpxd.event.burstFilter.compressToSyslog option.
      This option enables you to compress the bursting of events in the syslog server. The default value for the setting is disabled.

7. The burst settings are not visible with their default values in **Advanced Settings**. However, a key-value can be entered for the configuration to take effect.

   Note: Adding or modifying advanced settings might result in an unstable environment. Configuration parameters cannot be removed once they are added.

   a) Configure a key-value to enable the config.vpxd.event.burstFilter.enabled option.

      This parameter enables burst detection of the VC database and syslog. On disabling burst filter, bursts are not detected and the events are stored in the database or remote syslog server by default without compression. The default value is Enabled.

   b) Configure a key-value to enable the config.vpxd.event.burstFilter.rateEvents option.

      You can configure the number of events after which a burst is detected. If the configured limit is reached, the event sequence is considered a burst and is compressed while storing it in the VC database. The default value is 30. If the default is set, then the first 30 events are not compressed. They are used to detect a burst. If a burst is detected, then a single consolidated event with their count replaces the subsequent events after the first 30 events.

      Note: It does not compress the real-time stream of events like alarms and `EventManager` property collector updates.

   c) Configure a key-value to enable the config.vpxd.event.burstFilter.rateSeconds option.

      This parameter allows you to configure the number of seconds the data is stored for an event from the last time the event occurred. Higher values load the burst filter cache, and the bursts are detected even if the incoming flow of events is not even. Lower values exert lesser load on burst filter cache, and bursts may not be detected if there is a temporary halt of incoming events. The default value is 30 seconds.

   d) Configure a key-value to enable the config.vpxd.event.burstFilter.cacheSize option.

      The number of unique events tracked by the burst filter. When the cache is full, the burst filter stops monitoring the incoming new unique events and passes them through the VC database and syslog. The default value is 128000.

      Note: Setting a lower value than default reduces the memory footprint but it also reduces the capacity to detect bursts for a large inventory.

   e) Configure a key-value to enable the config.vpxd.event.burstFilter.whitelist option.

      You can configure the burst filter to compress all types of events except the events that are on the allow list. This parameter allows you to separate event types. It can avoid in monitoring few event types by the burst filter. The default value is `<whiteList>vim.event.UserLoginSessionEvent;vim.event.UserLogoutSessionEvent</whiteList>`

   f) Configure a key-value to enable the config.vpxd.event.burstFilter.compressRatio option.

      When the burst filter starts compressing an event, it posts a compressed event when the burst ends or on every X event. If a burst occurs for days, it posts some events instead of muting them all until the burst ends. The default value is 3600. The events are logged every 3600 events.

   Note: Restart the `vmware-vpxd` service for all changes to take effect. For more information how to restart services in the vSphere Client, see *vCenter Server and Host Management documentation*.

Streaming Events to a Remote Syslog Server

After you enable remote streaming, vCenter Server starts streaming and only the newly generated events are streamed to the remote syslog server.

All syslog messages begin with a specific prefix. You can distinguish the vCenter Server events from other syslog messages by their `Event` prefix.

The syslog protocol limits the length of syslog messages to 1024 characters. Messages that are longer than 1024 characters split into multiple syslog messages.

In the syslog server, events have the following format:

```
<syslog-prefix> : Event [eventId] [partInfo] [createdTime] [eventType] [severity] [user]
 [target] [chainId] [desc]
```

Item	Description
syslog-prefix	Displays the syslog prefix. The <*syslog-prefix*> is determined by the remote syslog server configuration.
eventId	Displays the unique ID of the event message. The default value is Event.
partInfo	Displays whether the message is split into parts.
createdTime	Displays the time when the event was generated.
eventType	Displays the event type.
severity	Displays whether the event is a piece information, a warning, or an error.
user	Displays the name of the user who generated the event.
target	Displays the object the event refers to.
chainId	Displays information about the parent or the group ID.
desc	Displays the description of the event.

Split of Long Event Message into Multiple Syslog Messages

Events that are longer than 1024 characters split into multiple syslog messages in the following manner:

```
<syslog-prefix> : Event [eventId][1-X][payload-part-1]<syslog-prefix> : Event [eventId][2-X][pay-
load-part-2]
...
<syslog-prefix> : Event [eventId][X-X][payload-part-X]
```

The *X* stands for the number of the event message parts.

Forward vCenter Server Log Files to Remote Syslog Server

You can forward the vCenter Server log files to a remote syslog server to conduct an analysis of your logs.

Log in to the vCenter Server Management Interface as root.

Note: ESXi can be configured to send log files to a vCenter Server rather than storing them to a local disk. The recommended maximum numbers of supported hosts to collect logs from is 30. See http://kb.vmware.com/s/article/2003322 for information on how to configure ESXi log forwarding. This feature is intended for smaller environments with stateless ESXi hosts. For all other cases, use a dedicated log server. Using vCenter Server to receive ESXi log files might impact vCenter Server performance.

1. In the vCenter Server Management Interface, select **Syslog**.
2. In the Forwarding Configuration section, click **Configure** if you have not configured any remote syslog hosts. Click **Edit** if you already have configured hosts.
3. In the Create Forwarding Configuration pane, enter the server address of the destination host. The maximum number of supported destination hosts is three.
4. From the **Protocol** drop-down menu, select the protocol to use.

Menu Item	Description
TLS	Transport Layer Security
TCP	Transmission Control Protocol
RELP	Reliable Event Logging Protocol
UDP	User Datagram Protocol

5. In the **Port** text box, enter the port number to use for communication with the destination host.
6. In the Create Forwarding Configuration pane, click **Add** to enter another remote syslog server.
7. Click **Save**.
8. Verify that the remote syslog server is receiving messages.
9. In the Forwarding Configuration section, click **Send Test Message.**
10. Verify on the remote syslog server that the test message was received.
    The new configuration settings are shown in the Forwarding Configuration section.

Configure Streaming of Events to a Remote Syslog Server

You can also configure writing of events to the vCenter Server streaming facility. Streaming events is supported only for the vCenter Server. The streaming of events to a remote syslog server is disabled by default. You can enable and configure the streaming of vCenter Server events to a remote syslog server from the vCenter Server Management Interface.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Expand **Settings** option, and select **Advanced Settings**.
4. Click **EDIT SETTINGS**.
5. Click on the filter text box present in the **Name** column of the table header. Type `vpxd.event`, and press Enter.
6. Enable or disable the vpxd.event.syslog.enabled option.
   By default, this option is enabled.
7. Click **SAVE**.

Retention of Events in the vCenter Server Database

You can configure vCenter Server to retain events in the database for a limited period. Discarding events periodically ensures optimal performance of the database.

In new installations of vCenter Server 6.5, the event clean up option is enabled by default and the default number of days to retain event messages in the database is 30. You can change this value to the number of days that you want to retain the event messages in the database.

If you are upgrading or migrating from vCenter Server6.7 or earlier, and you had the event cleanup option enabled, your setting to retain events is preserved after the upgrade or migration to vCenter Server 6.5.

After the retention period ends, the events are deleted from the database. However, there might be latency in the deletion of the events that are older than the configured retention setting.

Configure Database Settings

You can configure the maximum number of database connections that can occur simultaneously. To limit the growth of the vCenter Server database and save storage space, you can configure the database to discard information about tasks or events periodically.

Note: Do not use the database retention options, if you want to keep a complete history of tasks and events for your vCenter Server.

1. In the vSphere Client, navigate to the vCenter Server instance.
2. Select the **Configure** tab.
3. Under **Settings**, select **General**.
4. Click **Edit**.
5. In Edit vCenter general settings window, click **Database**.
6. In **Maximum connections** field, enter the required number of connections.

   Note: Do not change this value unless one of these issues exists in your system.

   - If your vCenter Server system performs many operations frequently and performance is critical, increase the number of connections.
   - If the database is shared and connections to the database are costly, decrease the number of connections.
7. Enable **Task cleanup** option for vCenter Server to delete the retained tasks periodically.
8. Optional: In **Task retention (days)** field, enter a value (in days).

   Information about tasks that are performed on this vCenter Server system is discarded after the specified number of days.
9. Enable **Event cleanup** option for vCenter Server to clean up the retained events periodically.
10. Optional: In **Event retention (days)** field, enter a value (in days).

    Information about events for this vCenter Server system is discarded after the specified number of days.

    Note: Monitor vCenter Server database consumption and disk partition in the vCenter Server Management Interface.

    Warning: Increasing the events retention to more than 30 days results in significant increase of vCenter database size and can shutdown the vCenter Server. Ensure that you increase the vCenter database accordingly.
11. Restart the vCenter Server to apply changes manually.
12. Click **SAVE**.

View Triggered Alarms

Triggered alarms are visible in several locations throughout the vSphere Client.

1. To view alarms triggered on a selected inventory object, click the **Monitor** tab, click **Issues and Alarms**.
2. Click **Triggered Alarms**.

Live Refresh of Recent Tasks and Alarms

Live refresh for recent tasks and alarms that result from operations that other users perform in your environment is enabled by default. Now, all recent tasks and alarms are visible to all of the users with permissions to view them.

Set an Alarm in the vSphere Client

In the vSphere Client you define alarms in the alarm definition wizard. You access the alarm definition wizard from the **Configure** tab, under **More**.

Create or Edit Alarms

To monitor your environment, you can create alarm definitions in the vSphere Client . You can access alarm definitions in the **Configure** tab.

Required Privilege: **Alarms** > **Create alarm** or **Alarms** > **Modify alarm**

Create alarms in the **Configure** tab.

1. Select an inventory object, click the **Configure** tab, and click **More**.
2. Click **Alarm Definitions**.
3. Click **Add** to add an alarm.
4. Select an alarm, click **Enable** to enable an alarm.
5. Select an alarm, click **Disable** to disable an alarm.
6. Select an alarm, click **Delete** to delete an alarm.
7. Click **Edit** to edit an alarm.
8. You can also edit an alarm definition by selecting **Monitor > Triggered Alarms**
   a) Select an alarm listed under **Alarm Name**.
   b) Click **Edit Alarm Definition** to edit an alarm.

Specify Alarm Name, Description, and Target

Settings of an alarm definition include alarm name, description, and target.

- Required Privilege: **Alarms** > **Create alarm** or **Alarms** > **Modify alarm**
- In the Alarms Definitions page, click Add. See Create an Alarm

1. Type a name and description.
2. Select the type of inventory object that this alarm monitors from the **Target type** drop-down menu

   Depending on the type of target that you choose to monitor, the summary that follows the **Target**, change.
3. Click **Next**.

   Note: Depending on the type of activity that you choose to monitor, the options on the Alarm Rule page, change.

Set alarm rule.

Specify Alarm Rules

You can select and configure the events, states, or conditions that trigger the alarm from the **Alarm Rule** page in the **New Alarm Definition** wizard.

Required Privilege: **Alarms** > **Create alarm** or **Alarms** > **Modify alarm**

An alarm definition must contain at least one trigger before you can save it.

1. Select a trigger from the drop-down menu.

   The combined event triggers are displayed. You can set the rule for a single event only. You must create multiple rules for multiple events.

2. Click **Add Argument** to select an argument from the drop-down menu.

   It supports **ALL** based expression, option to select **ANY** is not available. You must create a separate alarm definition for each trigger. The **OR** operator is not supported in the vSphere Client. However, you can combine more than one condition trigger with **AND** operator.

3. Select an operator from the drop-down menu.
4. Select an option from the drop-down menu to set the threshold for triggering an alarm
5. Select severity of the alarm from the drop-down menu.

   You can set the condition to either **Show as Warning** or **Show as Critical**, but not for both. You must create a separate alarm definition for warning and critical status. **Keep the target's current state** option can be enabled only for an event based alarm condition. For example, if **Cannot power off the VM** and **Keep the target's current state** is selected for an alarm rule, then it cannot be combined with any other alarm rule with different severities like **Warning** or **Critical**. These alarms will not have reset rules as the alarm rule does not change the state of the target object.

6. Send email notifications
   a) To send email notifications when alarms are triggered, enable **Send email notifications**.
   b) In the **Email to**, enter recipient addresses. Use commas to separate multiple addresses.
7. To send traps when alarms are triggered on a vCenter Server instance, enable **Send SNMP traps**.
8. Run scripts
   a) To run scripts when alarms are triggered, enable **Run script**.
   b) In **Run this script** column, enter the full path to the script.

      ```
      /var/myscripts/myAlarmActionScript
      ```

      You can use environment variables to define more complex scripts and attach them to multiple alarms or inventory objects so that the alarm action occurs when the alarm triggers.

Table 495: Alarm Environment Variables

Variable Name	Variable Description	Supported Alarm Type
VMWARE_ALARM_NAME	Name of the triggered alarm.	Condition, State, Event
VMWARE_ALARM_ID	MOID of the triggered alarm.	Condition, State, Event
VMWARE_ALARM_TARGET_NAME	Name of the entity on which the alarm triggered.	Condition, State, Event
VMWARE_ALARM_TARGET_ID	MOID of the entity on which the alarm triggered.	Condition, State, Event
VMWARE_ALARM_OLDSTATUS	Old status of the alarm.	Condition, State, Event
VMWARE_ALARM_NEWSTATUS	New status of the alarm.	Condition, State, Event
VMWARE_ALARM_TRIGGERINGSUMMARY	Multiline summary of the alarm.	Condition, State, Event
VMWARE_ALARM_DECLARINGSUMMARY	Single-line declaration of the alarm expression.	Condition, State, Event

Variable Name	Variable Description	Supported Alarm Type
VMWARE_ALARM_ALARMVALUE	Value that triggered the alarm.	Condition, State
VMWARE_ALARM_EVENTDESCRIPTION	Description text of the alarm status change event.	Condition, State
VMWARE_ALARM_EVENTDESCRIPTION	Description of the event that triggered the alarm.	Event
VMWARE_ALARM_EVENT_USERNAME	User name associated with the event.	Event
VMWARE_ALARM_EVENT_DATACENTER	Name of the datacenter in which the event occurred.	Event
VMWARE_ALARM_EVENT_COMPUTERESOURCE	Name of the cluster or resource pool in which the event occurred.	Event
VMWARE_ALARM_EVENT_HOST	Name of the host on which the event occurred.	Event
VMWARE_ALARM_EVENT_VM	Name of the virtual machine on which the event occurred.	Event
VMWARE_ALARM_EVENT_NETWORK	Name of the network on which the event occurred.	Event
VMWARE_ALARM_EVENT_DATASTORE	Name of the datastore on which the event occurred.	Event
VMWARE_ALARM_EVENT_DVS	Name of the vNetwork Distributed Switch on which the event occurred.	Event

If your script does not make use of the alarm environment variables, include any necessary parameters in the configuration field. Enclose parameters in curly brackets. For example:

```
/var/myscripts/myAlarmActionScript {alarmName} {targetName}
```

Check that the script can be executed:

```
chmod +x /var/myscripts/myAlarmActionScript
```

9. (Optional) Configure alarm transitions and frequency.
10. Select an advanced action from the drop-down menu.

    You can define the advanced actions for virtual machine and hosts. These advanced actions are applicable only for virtual machines and hosts. There are different sets of advanced actions based on target types of virtual machines and hosts.

    You can add multiple advanced actions for an alarm.
11. (Optional) Configure frequency for advanced actions.
12. Click **Add Another Rule** to add an additional rule for an alarm.
13. Click **Duplicate Rule** to create an identical rule for an alarm.
14. Click **Remove Rule** to remove an existing rule set for an alarm.

Click **Next** to set the Reset Rule.

Specify Alarm Reset Rules

You can select and configure the events, states, or conditions that trigger the alarm from the **Reset Rule** page in the **New Alarm Definition** wizard.

Required Privilege: **Alarms** > **Create alarm** or **Alarms** > **Modify alarm**

You can set the Alarm Reset Rule

1. Enable the **Reset the alarm to green** option.
2. Select a trigger from the drop-down menu.

   The combined event triggers are displayed. You can set the rule for a single event only. You must create multiple rules for multiple events.
3. Click **Add Argument** to select an argument from the drop-down menu.

   It supports **ALL** based expression, option to select **ANY** is not available. You must create a separate alarm definition for each trigger. The **OR** operator is not supported in the vSphere Client. However, you can combine more than one condition trigger with **AND** operator.
4. Select an operator from the drop-down menu.
5. Send email notifications
   a) To send email notifications when alarms are triggered, enable **Send email notifications**.
   b) In the **Email to**, enter recipient addresses. Use commas to separate multiple addresses.
6. To send traps when alarms are triggered on a vCenter Server instance, enable **Send SNMP traps**.
7. Run scripts
   a) To run scripts when alarms are triggered, enable **Run script**.
   b) In **Run this script** column, type script or command information:

      If your script does not make use of the alarm environment variables, include any necessary parameters in the configuration field. Enclose parameters in curly brackets. For example:

      ```
      c:\tools\cmd.exe {alarmName} {targetName}
      c:\windows\system32\cmd.exe /c c:\tools\cmd.bat {alarmName} {targetName}
      ```

      The script can run on any platform. You must provide the path to the script and argument keys. For example:

      ```
      /var/myscripts/myAlarmActionScript {alarmName} {targetName}
      ```
8. (Optional) Configure alarm transitions and frequency.
9. Select an advanced action from the **Add Advanced Actions** drop-down menu.

   You can add multiple advanced actions for an alarm reset rule. You can define the advanced actions for virtual machines and hosts. These advanced actions are applicable only for virtual machines and hosts. There are different sets of advanced actions based on target types of virtual machines and hosts.

   You can add multiple advanced actions for an alarm.
10. (Optional) Configure frequency for advanced actions.
11. Click **Add Another Rule** to add an additional reset rule for an alarm.
12. Click **Duplicate Rule** to create an identical reset rule for an alarm.
13. Click **Remove Rule** to remove an existing reset rule set for an alarm.

    Click **Next** to review the alarm definition.

Review and Enable Alarm

You can review and enable the alarm in the vSphere Client

Required Privilege: **Alarms** > **Create alarm** or **Alarms** > **Modify alarm**

After setting the alarm rule, review the alarm before enabling the alarm.

1. Review the **Alarm Name**, **Description**, **Targets**, and **Alarm Rule**.
2. (Optional) Configure alarm transitions and frequency.
3. Select **Enable this alarm** to enable the alarm.

The alarm is enabled.

Disable Alarms on Specific Objects

vSphere includes a feature to disable alarms on specific leaf object in the inventory, even if those are defined on one of its parents. This feature is helpful, if a specific alarm is not applicable for a given object.

Required Privilege: Alarms.Disable or enable alarm on entity

You can access alarms in the **Configure** tab.

Note: UI automatically enables "Disable/Enable" buttons for alarm specific leaf entities.

1. Select an inventory object, click the **Configure** tab, and click **More**.
2. Click **Alarm Definitions**.
3. Select an **Alarm**.
4. Click **Disable** to disable the alarm on that entity.

Acknowledge Triggered Alarms

After you acknowledge an alarm in the vSphere Client, its alarm actions are discontinued. Alarms are not cleared, or reset when acknowledged.

Required privilege: **Alarm** > **Alarm Acknowledge**

Acknowledging an alarm lets other users know that you are taking ownership of the issue. For example, a host has an alarm set to monitor CPU usage. It sends an email to an administrator when the alarm is triggered. The host CPU usage spikes, triggering the alarm which sends an email to the host's administrator. The administrator acknowledges the triggered alarm to let other administrators know the problem is being addressed, and to prevent the alarm from sending more email messages. The alarm, however, is still visible in the system.

- Right-click the alarm in the Alarms panel and select **Acknowledge**.
- Acknowledge the alarm in the **Monitor** tab.
  a) Select an inventory object in the object navigator.
  b) Click the **Monitor** tab.
  c) Click **Issues and Alarms**, and click **Triggered Alarms**.
  d) Select an alarm and select **Acknowledge**.

Reset Triggered Event Alarms

An alarm triggered by an event might not reset to a normal state if vCenter Server does not retrieve the event that identifies the normal condition. In such cases, reset the alarm manually in the vSphere Client to return it to a normal state.

Required privilege: **Alarm** > **Set Alarm Status**

- Right-click an alarm in the Alarms sidebar pane and select **Reset to green**.
- Reset triggered alarms in the **Monitor** tab.
  a) Select an inventory object.
  b) Click the **Monitor** tab.
  c) Click **Issuesand Alarms**, and click **Triggered Alarms**.
  d) Select the alarms you want to reset.
     Use Shift+left-click or Ctrl+left-click to select multiple alarms is supported in the vSphere Client.
  e) Right-click an alarm and select **Reset to Green**.

Monitoring Solutions with the vCenter Solutions Manager

A solution is an extension of vCenter Server that adds new functions to the vCenter Server instance. In the vSphere Client, you can view an inventory of the installed solutions with their detailed information. You can also monitor the health status of the solutions.

VMware products that integrate with vCenter Server are also considered solutions. For example, vSphere ESX Agent Manager is a VMware solution that lets you manage host agents that add new capabilities to ESX and ESXi hosts.

You can also install a solution to add functionality from third-party technologies to the standard functions of vCenter Server. Solutions are typically delivered as OVF packages. You can install and deploy solutions from the vSphere Client. You can integrate the solutions into the vCenter Solutions Manager, which provides a list of all installed solutions.

If a virtual machine or vApp runs a solution, a custom icon represents it in the inventory of the vSphere Client. Each solution registers a unique icon to show that the solution manages the virtual machine or vApp. The icons show the power states (powered on, paused, or powered off). Solutions display more than one type of icon if they manage more than one type of virtual machine or vApp.

When you power on or power off a virtual machine or vApp, you are notified that you are operating with an object that is managed by the vCenter Solutions Manager. When you attempt another operation on a virtual machine or a vApp that is managed by a solution, an informational warning message appears.

For more information, see the *Developing and Deploying vSphere Solutions, vServices, and ESX Agents* documentation.

View Solutions

vCenter Solutions Manager helps to deploy, monitor, and interact with solutions that are installed in a vCenter Server instance.

The vCenter Solutions Manager displays information about the solution, such as the solution name, the vendor name, and the version of the product. The vCenter Solutions manager also displays information about the health of a solution.

1. Navigate to the vCenter Solutions Manager.
   a) In the vSphere Client, select **Menu** > **Administration**.
   b) Expand **Solutions** and click **vCenter Server Extensions**.
2. Click a solution from the list.

   For instance, vService Manager or vSphere ESX Agent Manager.
3. Navigate through the tabs to view information about the solution.
   - **Summary**: You can view details about the solution, such as the product name, a short description, and links to the product and vendor websites. You can also view the solution configuration and the solution UI.
     Select the vCenter Server link to view the **Summary** page of the Virtual Machines or vApp.
   - **Monitor**: You can view the tasks and events related to the solution.
   - **VMs**: You can view a list of all the Virutal Machines and vApps that belong to the solution.

vSphere ESX Agent Manager

The vSphere ESX Agent Manager automates the process of deploying and managing ESX and ESXi agents, which extend the function of the host to provide additional services to a vSphere solution.

The vCenter Solutions Manager displays information about the vSphere ESX Agent Manager. The details include extension, related tasks and events, ESX agencies, agency related issues, and a list of the Virtual Machines and vApps that belong to the Agent Manager.

Monitor ESX Agent Health Status

The vCenter Solutions Manager displays the vSphere ESX Agent Manager that tracks the health status of agents on ESX/ESXi hosts.

vCenter Solutions Manager keeps track of whether the agents of a solution work as expected. Outstanding issues are reflected by the solution's ESX Agent Manager status and list of issues.

When there is a change in the current status of the solution's outstanding issues, the vCenter Solutions manager updates the ESX Agent Manager summary status and state. Administrators use this status to track whether the goal state is reached or not.

Table 496: ESX Agent Manager Health Status

Health Status Color	Description
Red	The solution must intervene for the ESX Agent Manager to proceed. For example, if a virtual machine agent is powered off manually on a compute resource and the ESX Agent Manager does not attempt to power on the agent. The ESX Agent Manager reports this action to the solution, and the solution alerts the administrator to power on the agent.
Yellow	The ESX Agent Manager is actively working to reach a goal state. The goal state can be enabled, disabled, or uninstalled. For example, when a solution is registered, its status is yellow until the ESX Agent Manager deploys the solutions agents to all the specified compute resources. A solution does not need to intervene when the ESX Agent Manager reports its ESX Agent Manager health status as yellow.
Green	A solution and all its agents have reached the goal state.

Resolve Agency Issues

ESX agencies provide an overview of all the issues related to ESX agents. You can resolve a single issue in the agency runtime information or you can resolve all issues at once.

ESX agencies are containers for ESX agents. ESX agencies aggregate information about the agents that they manage and all the issues that relate to those ESX agents.

1. Navigate to the vCenter Solutions Manager.
   a) In the vSphere Client, select **Menu** > **Administration**.
   b) Expand **Solutions** and click **vCenter Server Extensions**.
2. Select vSphere ESX Agent Manager and click the **Configure** tab.

   In the ESX Agencies pane, you can see a list of all agencies along with its cluster and solution information. You can click on a cluster name, to view the details of that cluster.

3. Select your task.
   - Resolve a single agency issue.
     a. Select an agency.
        Below the agency list, you can see a list of all the issues that are related to the selected agency.
     b. Select an issue from the list of issues for the selected agency.
     c. Click the vertical ellipsis icon and click **Resolve Issue**.
   - Resolve all agency issues.
     a. Select an agency.
     b. Click the vertical ellipsis icon and click **Resolve All Isues**.
        All the issues that are related to the selected agencies are resolved.

Monitoring the Health of Services and Nodes

You can monitor the health status of services and nodes to determine whether problems exist in your environment.

The vSphere Client provides an overview of all services and nodes across the management stack of the vCenter Server system. A list of default services is available for each vCenter Server instance.

View the Health Status of Nodes

In the vSphere Client, you can view the health status of vCenter Server nodes.

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

vCenter Server instances and machines that run vCenter Server services are considered nodes. Graphical badges represent the health status of nodes.

1. Use the vSphere Client to log in as administrator@*`your_domain_name`* to the vCenter Server instance.
   The address is of the type http://*`appliance-IP-address-or-FQDN`*/ui.
2. From the vSphere Client menu, select **Administration**.
3. Select **Deployment** > **System Configuration**.
4. Select a node to view its health status.

Table 497: Health States

Badge Icon	Description
	Good. The health of the object is normal.
	Warning. The object is experiencing some problems.
	Critical. The object is either not functioning properly or will stop functioning soon.
	Unknown. No data is available for this object.

View the Health Status of Services

You can view the health status of various vCenter Services using the vCenter Server Management Interface

- Verify that the vCenter Server is successfully deployed and running.
- If you are using Internet Explorer, verify that TLS 1.0, TLS 1.1, and TLS 1.2 are enabled in the security settings.

Note: The login session expires if you leave the vCenter Server Management Interface idle for 10 minutes.

1. In a Web browser, go to the vCenter Server Management Interface, https://*appliance-IP-address-or-FQDN*:5480.
2. Log in as root.
   The default root password is the password that you set while deploying vCenter Server.
3. In the vCenter Server Management Interface, click **Services**.
4. You can view the health of all the listed services in the **Health** column.

Performance Monitoring Utilities: resxtop and esxtop

The `resxtop` and `esxtop` command-line utilities provide a detailed look at how ESXi uses resources in real time. You can start either utility in one of three modes: interactive (default), batch, or replay.

The fundamental difference between `resxtop` and `esxtop` is that you can use `resxtop` remotely, whereas you can start `esxtop` only through the ESXi Shell of a local ESXi host.

Using the esxtop Utility

You can run the `esxtop` utility using the ESXi Shell to communicate with the management interface of the ESXi host. You must have root user privileges.

esxtop Utility

To use the `esxtop` utility, type the following command with desired options:

```
esxtop [-h] [-v] [-b] [-l] [-s] [-a] [-c config file] [-R vm-support_dir_path]  [-d delay] [-n iterations] [-export-entity entity-file] [-import-entity entity-file]
```

Command-Line Help Option	Description
`-h`	Prints this help menu.
`-v`	Prints version.
`-b`	Enables batch mode.
`-l`	Locks the esxtop objects to those available in the first snapshot.
`-s`	Enables secure mode.
`-a`	Displays all statistics.
`-c`	Sets the esxtop configuration file, which by default is `.esxtop60rc`.
`-R`	Enables replay mode.
`-d`	Sets the delay between updates in seconds.
`-n`	Runs esxtop for only n iterations. Use `-n infinity` to run esxtop for infinite period of time.
`-u`	Suppresses server-wide physical CPU statistics.

For example:

```
[root@localhost:~] esxtop
```

The above command will open the interactive screen of esxtop, by default.

```
[root@localhost:~] esxtop -b -a -d 10 -n 3 > /vmfs/volumes/localhost/test.csv
```

The above command runs the batch mode of esxtop with all counters, updates delay of 10 secs for 3 iterations. The output is written to the test.csv file which can be opened with other tools like Windows Perfmon.

esxtop Configuration

The `esxtop` utility reads its default configuration from `.esxtop50rc` on the ESXi system. This configuration file consists of nine lines.

The first eight lines contain lowercase and uppercase letters to specify which fields appear in which order on the CPU, memory, storage adapter, storage device, virtual machine storage, network, interrupt, and CPU power panels. The letters correspond to the letters in the Fields or Order panels for the respective `esxtop` panel.

The ninth line contains information on the other options. Most important, if you saved a configuration in secure mode, you do not get an insecure `esxtop` without removing the `s` from the seventh line of your `.esxtop50rc` file. A number specifies the delay time between updates. As in interactive mode, typing `c`, `m`, `d`, `u`, `v`, `n`, `I`, or `p` determines the panel with which `esxtop` starts.

Note: Do not edit the `.esxtop50rc` file. Instead, select the fields and the order in a running `esxtop` process, make changes, and save this file using the `W` interactive command.

Related Links

Interactive Mode Command-Line Options on page 3264

You can use various command-line options with `esxtop` and `resxtop` in interactive mode.

Using the resxtop Utility

`resxtop` is a command-line utility or tool that runs on linux and provides a detailed look at how ESXi uses resources in real time.

Before you can use any `resxtop` commands, you must download and install `resxtop` to your system.

Note: `resxtop` is supported only on Linux.

After it is set up, start `resxtop` from the command line. For remote connections, you can connect to a host either directly or through vCenter Server.

To launch `resxtop` and connect to a remote server, enter this command

```
resxtop --server <hostname> --username <user>
```

The command-line options listed in the following table are the same as for `esxtop` (except for the `R` option) with additional connection options.

Note: `resxtop` does not use all the options shared by other ESXCLI commands.

Table 498: resxtop Command-Line Options

Option	Description
`[server]`	Name of the remote host to connect to (required). If connecting directly to the ESXi host, use the name of that host. If your connection to the ESXi host is indirect (that is, through vCenter Server), use the name of the vCenter Server system for this option.

Option	Description
[vihost]	If you connect indirectly (through vCenter Server), this option should contain the name of the ESXi host you connect to. If you connect directly to the host, this option is not used. Note that the host name needs to be the same as what appears in the vSphere Client.
[portnumber]	Port number to connect to on the remote server. The default port is 443, and unless this is changed on the server, this option is not needed.
[username]	User name to be authenticated when connecting to the remote host. The remote server prompts you for a password.

You can also use `resxtop` on a local ESXi host by omitting the `server` option on the command line. The command defaults to localhost.

Installing resxtop on Ubuntu Linux

Installing RESXTOP on Linux systems is a simple process the involves extracting the files from the archive, running and install script, and updating the path.

1. Download `resxtop` from https://code.vmware.com/web/tool/7.0/resxtop.
2. Unpack the archive using the linux tar command `"tar -xvf resxtop-7.0.0-15992393-lin64.tgz"`.
3. Execute the install script by running the linux command `"./install.sh"`.
4. Update the path by running the linux command `"export LD_LIBRARY_PATH=/usr/lib/vmware/resxtop"`.

Related Links

Interactive Mode Command-Line Options on page 3264

You can use various command-line options with `esxtop` and `resxtop` in interactive mode.

Using esxtop or resxtop in Interactive Mode

By default, `resxtop` and `esxtop` run in interactive mode. Interactive mode displays statistics in different panels.

A help menu is available for each panel.

Interactive Mode Command-Line Options

You can use various command-line options with `esxtop` and `resxtop` in interactive mode.

Table 499: Interactive Mode Command-Line Options

Option	Description
h	Prints help for `resxtop` (or `esxtop`) command-line options.
v	Prints `resxtop` (or `esxtop`) version number.
s	Calls `resxtop` (or `esxtop`) in secure mode. In secure mode, the `-d` command, which specifies delay between updates, is disabled.
d	Specifies the delay between updates. The default is five seconds. The minimum is two seconds. Change this with the interactive command `s`. If you specify a delay of less than two seconds, the delay is set to two seconds.
n	Number of iterations. Updates the display `n` times and exits. Default value is 10000.
server	The name of the remote server host to connect to (required for `resxtop` only).

Option	Description
vihost	If you connect indirectly (through vCenter Server), this option should contain the name of the ESXi host you connect to. If you connect directly to the ESXi host, this option is not used. Note that the host name needs to be the same as what is displayed in the vSphere Client.
portnumber	The port number to connect to on the remote server. The default port is 443, and unless this is changed on the server, this option is not needed. (resxtop only)
username	The user name to be authenticated when connecting to the remote host. The remote server prompts you for a password, as well (resxtop only).
a	Show all statistics. This option overrides configuration file setups and shows all statistics. The configuration file can be the default ~/.esxtop50rc configuration file or a user-defined configuration file.
c*filename*	Load a user-defined configuration file. If the -c option is not used, the default configuration filename is ~/.esxtop50rc. Create your own configuration file, specifying a different filename, using the W single-key interactive command.

Common Statistics Description

Several statistics appear on the different panels while resxtop (or esxtop) is running in interactive mode. These statistics are common across all four panels.

The Uptime line, found at the top of each of the four resxtop (or esxtop) panels, displays the current time, time since last reboot, number of currently running worlds and load averages. A world is an ESXi VMkernel schedulable entity, similar to a process or thread in other operating systems.

Below that the load averages over the past one, five, and fifteen minutes appear. Load averages consider both running and ready-to-run worlds. A load average of 1.00 means that there is full utilization of all physical CPUs. A load average of 2.00 means that the ESXi system might need twice as many physical CPUs as are currently available. Similarly, a load average of 0.50 means that the physical CPUs on the ESXi system are half utilized.

Statistics Columns and Order Pages

You can define the order of fields displayed in interactive mode.

If you press f, F, o, or O, the system displays a page that specifies the field order on the top line and short descriptions of the field contents. If the letter in the field string corresponding to a field is uppercase, the field is displayed. An asterisk in front of the field description indicates whether a field is displayed.

The order of the fields corresponds to the order of the letters in the string.

From the Field Select panel, you can:

- Toggle the display of a field by pressing the corresponding letter.
- Move a field to the left by pressing the corresponding uppercase letter.
- Move a field to the right by pressing the corresponding lowercase letter.

Interactive Mode Single-Key Commands

When running in interactive mode, resxtop (or esxtop) recognizes several single-key commands.

All interactive mode panels recognize the commands listed in the following table. The command to specify the delay between updates is disabled if the s option is given on the command line. All sorting interactive commands sort in descending order.

Table 500: Interactive Mode Single-Key Commands

Key	Description
h or?	Displays a help menu for the current panel, giving a brief summary of commands, and the status of secure mode.
space	Immediately updates the current panel.
^L	Erases and redraws the current panel.
f or F	Displays a panel for adding or removing statistics columns (text boxes) to or from the current panel.
o or O	Displays a panel for changing the order of statistics columns on the current panel.
#	Prompts you for the number of statistics rows to display. Any value greater than 0 overrides automatic determination of the number of rows to show, which is based on window size measurement. If you change this number in one `resxtop` (or `esxtop`) panel, the change affects all four panels.
s	Prompts you for the delay between updates, in seconds. Fractional values are recognized down to microseconds. The default value is five seconds. The minimum value is two seconds. This command is not available in secure mode.
W	Write the current setup to an esxtop (or resxtop) configuration file. This is the recommended way to write a configuration file. The default filename is the one specified by -c option, or `~/.esxtop50rc` if the -c option is not used. You can also specify a different filename on the prompt generated by this W command.
q	Quit the interactive mode.
c	Switch to the CPU resource utilization panel.
p	Switch to the CPU Power utilization panel.
m	Switch to the memory resource utilization panel.
d	Switch to the storage (disk) adapter resource utilization panel.
u	Switch to storage (disk) device resource utilization screen.
v	Switch to storage (disk) virtual machine resource utilization screen.
n	Switch to the network resource utilization panel.
i	Switch to the interrupt panel.

CPU Panel

The CPU panel displays server-wide statistics as well as statistics for the individual world, resource pool, and virtual machine CPU utilization.

Resource pools, virtual machines that are running, or other worlds are at times called groups. For worlds belonging to a virtual machine, statistics for the virtual machine that is running are displayed. All other worlds are logically aggregated into the resource pools that contain them.

Table 501: CPU Panel Statistics

Line	Description
PCPU USED(%)	A PCPU refers to a physical hardware execution context. It can be a physical CPU core if the hyperthreading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) if the hyperthreading is enabled. PCPU USED(%) displays the following percentages: • percentage of CPU usage per PCPU • percentage of CPU usage averaged over all PCPUs

Line	Description
	CPU Usage (%USED) is the percentage of PCPU nominal frequency that was used since the last screen update. It equals the total sum of %USED for Worlds that ran on this PCPU. **Note:** If a PCPU is running at frequency that is higher than its nominal (rated) frequency, then PCPU USED(%) can be greater than 100%. If a PCPU and its partner are busy when hyperthreading is enabled, each PCPU account for half of the CPU usage.
PCPU UTIL(%)	A PCPU refers to a physical hardware execution context. It can be a physical CPU core if the hyperthreading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) if the hyperthreading is enabled. PCPU UTIL(%) represents the percentage of real time that the PCPU was not idle (raw PCPU utilization). It displays the percentage CPU utilization per PCPU, and the percentage CPU utilization averaged over all PCPUs. **Note:** PCPU UTIL(%) might differ from PCPU USED(%) due to power management technologies or hyperthreading.
ID	Resource pool ID or virtual machine ID of the resource pool or virtual machine of the world that is running. Alternatively, the world ID of the world that is running.
GID	Resource pool ID of the resource pool or virtual machine of the world that is running.
NAME	Name of the resource pool or virtual machine of the world that is running, or name of the world that is running.
NWLD	Number of members in the resource pool or virtual machine of the world that is running. If a Group is expanded using the interactive command `e` , then NWLD for all the resulting worlds is 1.
%STATE TIMES	Set of CPU statistics made up of the following percentages. For a world, the percentages are a percentage of one physical CPU core.
%USED	Percentage of physical CPU core cycles used by the resource pool, virtual machine, or world. %USED might depend on the frequency with which the CPU core is running. When running with lower CPU core frequency, %USED can be smaller than %RUN. On CPUs which support the turbo mode, CPU frequency can also be higher than the nominal (rated) frequency, and %USED can be larger than %RUN. %USED = %RUN + %SYS - %OVRLP
%SYS	Percentage of time spent in the ESXi VMkernel on behalf of the resource pool, virtual machine, or world to process interrupts and to perform other system activities. This time is part of the time used to calculate %USED. %USED = %RUN + %SYS - %OVRLP
%WAIT	Percentage of time the resource pool, virtual machine, or world spent in the blocked or busy wait state. This percentage includes the percentage of time the resource pool, virtual machine, or world was idle. 100% = %RUN + %RDY + %CSTP + %WAIT
%VMWAIT	The total percentage of time the Resource Pool/World spent in a blocked state waiting for events.
%IDLE	Percentage of time the resource pool, virtual machine, or world was idle. Subtract this percentage from %WAIT to see the percentage of time the resource pool, virtual machine, or world was waiting for some event. The difference, %WAIT- %IDLE, of the VCPU worlds can be used to estimate guest I/O wait time. To find the VCPU worlds, use the single-key command `e` to expand a virtual machine and search for the world NAME starting with "vcpu". (The VCPU worlds might wait for other events in addition to I/O events, so this measurement is only an estimate.)
%RDY	Percentage of time the resource pool, virtual machine, or world was ready to run, but was not provided CPU resources on which to execute. 100% = %RUN + %RDY + %CSTP + %WAIT
%MLMTD (max limited)	Percentage of time the ESXi VMkernel deliberately did not run the resource pool, virtual machine, or world because doing so would violate the resource pool, virtual machine, or world's limit setting. Because the resource pool, virtual machine, or world is ready to run when it is prevented from running in this way, the %MLMTD (max limited) time is included in %RDY time.

Line	Description
%SWPWT	Percentage of time a resource pool or world spends waiting for the ESXi VMkernel to swap memory. The %SWPWT (swap wait) time is included in the %WAIT time.
EVENT COUNTS/s	Set of CPU statistics made up of per second event rates. These statistics are for VMware internal use only.
CPU ALLOC	Set of CPU statistics made up of the following CPU allocation configuration parameters.
AMIN	Resource pool, virtual machine, or world attribute Reservation.
AMAX	Resource pool, virtual machine, or world attribute Limit. A value of -1 means unlimited.
ASHRS	Resource pool, virtual machine, or world attribute Shares.
SUMMARY STATS	Set of CPU statistics made up of the following CPU configuration parameters and statistics. These statistics apply only to worlds and not to virtual machines or resource pools.
AFFINITY BIT MASK	Bit mask showing the current scheduling affinity for the world.
HTSHARING	Current hyperthreading configuration.
CPU	The physical or logical processor on which the world was running when `resxtop` (or `esxtop`) obtained this information.
HTQ	Indicates whether the world is quarantined or not. N means no and Y means yes.
TIMER/s	Timer rate for this world.
%OVRLP	Percentage of system time spent during scheduling of a resource pool, virtual machine, or world on behalf of a different resource pool, virtual machine, or world while the resource pool, virtual machine, or world was scheduled. This time is not included in %SYS. For example, if virtual machine A is being scheduled and a network packet for virtual machine B is processed by the ESXi VMkernel, the time spent appears as %OVRLP for virtual machine A and %SYS for virtual machine B. %USED = %RUN + %SYS - %OVRLP
%RUN	Percentage of total time scheduled. This time does not account for hyperthreading and system time. On a hyperthreading enabled server, the %RUN can be twice as large as %USED. %USED = %RUN + %SYS - %OVRLP 100% = %RUN + %RDY + %CSTP + %WAIT
%CSTP	Percentage of time a resource pool spends in a ready, co-deschedule state. **Note:** You might see this statistic displayed, but it is intended for VMware use only. 100% = %RUN + %RDY + %CSTP + %WAIT
POWER	Current CPU power consumption for a resource pool (in Watts).
%LAT_C	Percentage of time the resource pool or world was ready to run but was not scheduled to run because of CPU resource contention.
%LAT_M	Percentage of time the resource pool or world was ready to run but was not scheduled to run because of memory resource contention.
%DMD	CPU demand in percentage. It represents the average active CPU load in the past minute.
CORE UTIL(%)	Percentage of CPU cycles per core when at least one of the PCPUs in this core is unhalted, and its average over all cores. This statistic only appears when hyperthreading is enabled. In batch mode, the corresponding CORE UTIL(%) statistic is displayed for each PCPU. For example, PCPU 0 and PCPU 1 have the same the CORE UTIL(%) number, and that is the number for core 0.

You can change the display using single-key commands.

Table 502: CPU Panel Single-Key Commands

Command	Description
e	Toggles whether CPU statistics are displayed expanded or unexpanded. The expanded display includes CPU resource utilization statistics broken down by individual worlds belonging to a resource pool or virtual machine. All percentages for the individual worlds are percentage of a single physical CPU. Consider these examples: • If the %Used by a resource pool is 30% on a two-way server, the resource pool is utilizing 30 percent of one physical core. • If the %Used by a world belonging to a resource pool is 30 percent on a two-way server, that world is utilizing 30% of one physical core.
U	Sorts resource pools, virtual machines, and worlds by the resource pool's or virtual machine's %Used column. This is the default sort order.
R	Sorts resource pools, virtual machines, and worlds by the resource pool's or virtual machine's %RDY column.
N	Sorts resource pools, virtual machines, and worlds by the GID column.
V	Displays virtual machine instances only.
L	Changes the displayed length of the NAME column.

CPU Power Panel

The CPU Power panel displays CPU Power utilization statistics.

On the CPU Power panel, statistics are arranged per physical CPU. A physical CPU is a physical hardware execution context. It is the physical CPU core when hyper-threading is unavailable or disabled, or a logical CPU (LCPU or SMT thread) when hyper-threading is enabled.

Table 503: CPU Power Panel Statistics

Line	Description
Power Usage	Current total power usage (in Watts).
Power Cap	Total power cap (in Watts).
PSTATE MHZ	Clock frequency per state.
%USED	Percentage of physical CPU nominal frequency used since the last screen update. It is the same as PCPU USED(%) shown in the CPU Screen.
%UTIL	Raw physical CPU utilization is the percentage of time that physical CPU was not idle. It is the same as PCPU UTIL(%) shown in the CPU Screen.
%Cx	Percentage of time the physical CPU spent in C-State 'x'.
%Px	Percentage of time the physical CPU spent in P-State 'x'. On systems with Processor Clocking Control, P-states are not directly visible to ESXi. The `esxtop` shows the percentage of time spent at full speed under the heading 'P0' and the percentage of time spent at any lower speed under 'P1'.
%Tx	Percentage of time the physical CPU spent in T-State 'x'.
%A/MPERF	aperf and mperf are two hardware registers used to keep track of the actual frequency and nominal frequency of the processor. Displays the real-time aperf to mperf ratio in the last esxtop update period. %A/MPERF *nominal frequency of the processor = current frequency of the processor

Memory Panel

The Memory panel displays server-wide and group memory utilization statistics. As on the CPU panel, groups correspond to resource pools, running virtual machines, or other worlds that are consuming memory.

The first line, found at the top of the Memory panel displays the current time, time since last reboot, number of currently running worlds, and memory overcommitment averages. The memory overcommitment averages over the past one, five, and fifteen minutes appear. Memory overcommitment of 1.00 means a memory overcommitment of 100 percent.

Table 504: Memory Panel Statistics

Field	Description	
PMEM (MB)	Displays the machine memory statistics for the server. All numbers are in megabytes.	
	total	Total amount of the machine memory in the server.
	vmk	Amount of the machine memory being used by the ESXi VMkernel.
	other	Amount of the machine memory being used by everything other than the ESXi VMkernel.
	free	Amount of the machine memory that is free.
VMKMEM (MB)	Displays the machine memory statistics for the ESXi VMkernel. All numbers are in megabytes.	
	managed	Total amount of the machine memory managed by the ESXi VMkernel.
	min free	Minimum amount of the machine memory that the ESXi VMkernel aims to keep free.
	rsvd	Total amount of the machine memory currently reserved by resource pools.
	ursvd	Total amount of the machine memory currently unreserved.
	state	Current machine memory availability state. Possible values are high, soft, hard and low. High means that the machine memory is not under any pressure and low means that it is.
NUMA (MB)	Displays the ESXi NUMA statistics. This line appears only if the ESXi host is running on a NUMA server. All numbers are in megabytes. For each NUMA node in the server, two statistics are displayed: • The total amount of machine memory in the NUMA node that is managed by ESXi. • The amount of machine memory in the node that is currently free (in parentheses). Shared memory for the ESXi host might be larger than the total amount of memory if memory is over-committed.	
PSHARE (MB)	Displays the ESXi page-sharing statistics. All numbers are in megabytes.	
	shared	Amount of the physical memory that is being shared.
	common	Amount of the machine memory that is common across worlds.
	saving	Amount of the machine memory that is saved because of page sharing. shared = common + saving

Field	Description
SWAP (MB)	Displays the ESXi swap usage statistics. All numbers are in megabytes. **curr** Current swap usage. **rclmtgt** Where the ESXi system expects the reclaimed memory to be. Memory can be reclaimed by swapping or compression. **r/s** Rate at which the memory is swapped in by the ESXi system from disk. **w/s** Rate at which the memory is swapped to disk by the ESXi system.
ZIP (MB)	Displays the ESXi memory compression statistics. All numbers are in megabytes. **zipped** Total compressed physical memory. **saved** Saved memory by compression.
MEMCTL (MB)	Displays the memory balloon statistics. All numbers are in megabytes. **curr** Total amount of the physical memory reclaimed using the `vmmemctl` module. **target** Total amount of physical memory the ESXi host attempts to reclaim using the `vmmemctl` module. **max** Maximum amount of the physical memory the ESXi host can reclaim using the `vmmemctl` module.
AMIN	Memory reservation for this resource pool or virtual machine.
AMAX	Memory limit for this resource pool or virtual machine. A value of -1 means Unlimited.
ASHRS	Memory shares for this resource pool or virtual machine.
NHN	Current home node for the resource pool or virtual machine. This statistic is applicable only on NUMA systems. If the virtual machine has no home node, a dash (-) appears.
NRMEM (MB)	Current amount of remote memory allocated to the virtual machine or resource pool. This statistic is applicable only on NUMA systems.
N% L	Current percentage of memory allocated to the virtual machine or resource pool that is local.
MEMSZ (MB)	Amount of physical memory allocated to a resource pool or virtual machine. The values are the same for the VMM and VMX groups. MEMSZ = GRANT + MCTLSZ + SWCUR + "never touched"
GRANT (MB)	Amount of guest physical memory mapped to a resource pool or virtual machine. The consumed host machine memory is equal to GRANT - SHRDSVD. The values are the same for the VMM and VMX groups.
CNSM	Amount of the memory currently consumed by the virtual machine. The memory currently consumed by the virtual machine is equal to the amount of memory that the VM guest operating system currently uses, excluding the amount of memory saved for sharing if memory sharing is enabled on the VM, excluding the amount of memory saved if some of the VM memory is compressed. For more information on memory sharing and memory compression, see the *vSphere Resource Management* documentation.
SZTGT (MB)	Amount of machine memory the ESXi VMkernel wants to allocate to a resource pool or virtual machine. The values are the same for the VMM and VMX groups.

Field	Description
TCHD (MB)	Working set estimate for the resource pool or virtual machine. The values are the same for the VMM and VMX groups.
%ACTV	Percentage of guest physical memory that is being referenced by the guest. This is an instantaneous value.
%ACTVS	Percentage of guest physical memory that is being referenced by the guest. This is a slow moving average.
%ACTVF	Percentage of guest physical memory that is being referenced by the guest. This is a fast moving average.
%ACTVN	Percentage of guest physical memory that is being referenced by the guest. This is an estimation. (You might see this statistic displayed, but it is intended for VMware use only.)
MCTL?	Memory balloon driver is installed or not. **N** means no, **Y** means yes.
MCTLSZ (MB)	Amount of physical memory reclaimed from the resource pool by way of ballooning.
MCTLTGT (MB)	Amount of physical memory the ESXi system attempts to reclaim from the resource pool or virtual machine by way of ballooning.
MCTLMAX (MB)	Maximum amount of physical memory the ESXi system can reclaim from the resource pool or virtual machine by way of ballooning. This maximum depends on the guest operating system type.
SWCUR (MB)	Current swap usage by this resource pool or virtual machine.
SWTGT (MB)	Target where the ESXi host expects the swap usage by the resource pool or virtual machine to be.
SWR/s (MB)	Rate at which the ESXi host swaps in memory from disk for the resource pool or virtual machine.
SWW/s (MB)	Rate at which the ESXi host swaps resource pool or virtual machine memory to disk.
LLSWR/s (MB)	Rate at which memory is read from the host cache. The reads and writes are attributed to the VMM group only, LLSWAP statistics are not displayed for the VM group.
LLSWW/s (MB)	Rate at which memory is written to the host cache from various sources. The reads and writes are attributed to the VMM group only, LLSWAP statistics are not displayed for the VM group.
CPTRD (MB)	Amount of data read from checkpoint file.
CPTTGT (MB)	Size of checkpoint file.
ZERO (MB)	Resource pool or virtual machine physical pages that are zeroed.
SHRD (MB)	Resource pool or virtual machine physical pages that are shared.
SHRDSVD (MB)	Machine pages that are saved because of resource pool or virtual machine shared pages.
OVHD (MB)	Current space overhead for resource pool.
OVHDMAX (MB)	Maximum space overhead that might be incurred by resource pool or virtual machine.
OVHDUW (MB)	Current space overhead for a user world. (You might see this statistic displayed, but it is intended for VMware use only.)
GST_NDx (MB)	Guest memory allocated for a resource pool on NUMA node x. This statistic is applicable on NUMA systems only.
OVD_NDx (MB)	VMM overhead memory allocated for a resource pool on NUMA node x. This statistic is applicable on NUMA systems only.
TCHD_W (MB)	Write working set estimate for resource pool.
CACHESZ (MB)	Compression memory cache size.
CACHEUSD (MB)	Used compression memory cache.

Field	Description
ZIP/s (MB/s)	Compressed memory per second.
UNZIP/s (MB/s)	Decompressed memory per second.

Table 505: Memory Panel Interactive Commands

Command	Description
M	Sort resource pools or virtual machines by MEMSZ column. This is the default sort order.
B	Sort resource pools or virtual machines by Group Memctl column.
N	Sort resource pools or virtual machines by GID column.
V	Display virtual machine instances only.
L	Changes the displayed length of the NAME column.

Storage Adapter Panel

Statistics in the Storage Adapter panel are aggregated per storage adapter by default. Statistics can also be viewed per storage path.

Table 506: Storage Adapter Panel Statistics

Column	Description
ADAPTR	Name of the storage adapter.
PATH	Storage path name. This name is only visible if the corresponding adapter is expanded. See interactive command e in Table 507: Storage Adapter Panel Interactive Commands.
NPTH	Number of paths.
AQLEN	Current queue depth of the storage adapter.
CMDS/s	Number of commands issued per second.
READS/s	Number of read commands issued per second.
WRITES/s	Number of write commands issued per second.
MBREAD/s	Megabytes read per second.
MBWRTN/s	Megabytes written per second.
RESV/s	Number of SCSI reservations per second.
CONS/s	Number of SCSI reservation conflicts per second.
DAVG/cmd	Average device latency per command, in milliseconds.
KAVG/cmd	Average ESXi VMkernel latency per command, in milliseconds.
GAVG/cmd	Average virtual machine operating system latency per command, in milliseconds.
QAVG/cmd	Average queue latency per command, in milliseconds.
DAVG/rd	Average device read latency per read operation, in milliseconds.
KAVG/rd	Average ESXi VMkernel read latency per read operation, in milliseconds.
GAVG/rd	Average guest operating system read latency per read operation, in milliseconds.

Column	Description
QAVG/rd	Average queue latency per read operation, in milliseconds.
DAVG/wr	Average device write latency per write operation, in milliseconds.
KAVG/wr	Average ESXi VMkernel write latency per write operation, in milliseconds.
GAVG/wr	Average guest operating system write latency per write operation, in milliseconds.
QAVG/wr	Average queue latency per write operation, in milliseconds.
FCMDS/s	Number of failed commands issued per second.
FREAD/s	Number of failed read commands issued per second.
FWRITE/s	Number of failed write commands issued per second.
FMBRD/s	Megabytes of failed read operations per second.
FMBWR/s	Megabytes of failed write operations per second.
FRESV/s	Number of failed SCSI reservations per second.
ABRTS/s	Number of commands cancelled per second.
RESETS/s	Number of commands reset per second.
PAECMD/s	The number of PAE (Physical Address Extension) commands per second.
PAECP/s	The number of PAE copies per second.
SPLTCMD/s	The number of split commands per second.
SPLTCP/s	The number of split copies per second.

The following table displays the interactive commands you can use with the storage adapter panel.

Table 507: Storage Adapter Panel Interactive Commands

Command	Description
`e`	Toggles whether storage adapter statistics appear expanded or unexpanded. Allows you to view storage resource utilization statistics broken down by individual paths belonging to an expanded storage adapter. You are prompted for the adapter name.
`r`	Sorts by READS/s column.
`w`	Sorts by WRITES/s column.
`R`	Sorts by MBREAD/s read column.
`T`	Sorts by MBWRTN/s written column.
`N`	Sorts first by ADAPTR column, then by PATH column. This is the default sort order.

Storage Device Panel

The storage device panel displays server-wide storage utilization statistics.

By default, the information is grouped per storage device. You can also group the statistics per path, per world, or per partition.

Table 508: Storage Device Panel Statistics

Column	Description
DEVICE	Name of the storage device.
PATH	Path name. This name is visible only if the corresponding device is expanded to paths. See the interactive command `p` in Table 509: Storage Device Panel Interactive Commands.
WORLD	World ID. This ID is visible only if the corresponding device is expanded to worlds. See the interactive command `e` in Table 509: Storage Device Panel Interactive Commands. The world statistics are per world per device.
PARTITION	Partition ID. This ID is visible only if the corresponding device is expanded to partitions. See interactive command `t` in Table 509: Storage Device Panel Interactive Commands.
NPH	Number of paths.
NWD	Number of worlds.
NPN	Number of partitions.
SHARES	Number of shares. This statistic is applicable only to worlds.
BLKSZ	Block size in bytes.
NUMBLKS	Number of blocks of the device.
DQLEN	Current device queue depth of the storage device.
WQLEN	World queue depth. This is the maximum number of ESXi VMkernel active commands that the world is allowed to have. This is a per device maximum for the world. It is valid only if the corresponding device is expanded to worlds.
ACTV	Number of commands in the ESXi VMkernel that are currently active. This statistic applies to only worlds and devices.
QUED	Number of commands in the ESXi VMkernel that are currently queued. This statistic applies to only worlds and devices.
%USD	Percentage of the queue depth used by ESXi VMkernel active commands. This statistic applies to only worlds and devices.
LOAD	Ratio of ESXi VMkernel active commands plus ESXi VMkernel queued commands to queue depth. This statistic applies to only worlds and devices.
CMDS/s	Number of commands issued per second.
READS/s	Number of read commands issued per second.
WRITES/s	Number of write commands issued per second.
MBREAD/s	Megabytes read per second.
MBWRTN/s	Megabytes written per second.
DAVG/cmd	Average device latency per command in milliseconds.
KAVG/cmd	Average ESXi VMkernel latency per command in milliseconds.
GAVG/cmd	Average guest operating system latency per command in milliseconds.
QAVG/cmd	Average queue latency per command in milliseconds.
DAVG/rd	Average device read latency per read operation in milliseconds.
KAVG/rd	Average ESXi VMkernel read latency per read operation in milliseconds.
GAVG/rd	Average guest operating system read latency per read operation in milliseconds.
QAVG/rd	Average queue read latency per read operation in milliseconds.

Column	Description
DAVG/wr	Average device write latency per write operation in milliseconds.
KAVG/wr	Average ESXi VMkernel write latency per write operation in milliseconds.
GAVG/wr	Average guest operating system write latency per write operation in milliseconds.
QAVG/wr	Average queue write latency per write operation in milliseconds.
ABRTS/s	Number of commands cancelled per second.
RESETS/s	Number of commands reset per second.
PAECMD/s	Number of PAE commands per second. This statistic applies to only paths.
PAECP/s	Number of PAE copies per second. This statistic applies to only paths.
SPLTCMD/s	Number of split commands per second. This statistic applies to only paths.
SPLTCP/s	Number of split copies per second. This statistic applies to only paths.

The following table displays the interactive commands you can use with the storage device panel.

Table 509: Storage Device Panel Interactive Commands

Command	Description
`e`	Expand or roll up storage world statistics. This command allows you to view storage resource utilization statistics separated by individual worlds belonging to an expanded storage device. You are prompted for the device name. The statistics are per world per device.
`P`	Expand or roll up storage path statistics. This command allows you to view storage resource utilization statistics separated by individual paths belonging to an expanded storage device. You are prompted for the device name.
`t`	Expand or roll up storage partition statistics. This command allows you to view storage resource utilization statistics separated by individual partitions belonging to an expanded storage device. You are prompted for the device name.
`r`	Sort by READS/s column.
`w`	Sort by WRITES/s column.
`R`	Sort by MBREAD/s column.
`T`	Sort by MBWRTN column.
`N`	Sort first by DEVICE column, then by PATH, WORLD, and PARTITION column. This is the default sort order.
`L`	Changes the displayed length of the DEVICE column.

Virtual Machine Storage Panel

This panel displays virtual machine-centric storage statistics.

By default, statistics are aggregated on a per-resource-pool basis. One virtual machine has one corresponding resource pool, so the panel displays statistics on a per-virtual-machine basis. You can also view the statistics on per-VSCSI-device basis.

Table 510: Virtual Machine Storage Panel Statistics

Column	Description
ID	Resource pool ID or VSCSI ID of VSCSI device.
GID	Resource pool ID.
VMNAME	Name of the resource pool.
VSCSINAME	Name of the VSCSI device.
NDK	Number of VSCSI devices
CMDS/s	Number of commands issued per second.
READS/s	Number of read commands issued per second.
WRITES/s	Number of write commands issued per second.
MBREAD/s	Megabytes read per second.
MBWRTN/s	Megabytes written per second.
LAT/rd	Average latency (in milliseconds) per read.
LAT/wr	Average latency (in milliseconds) per write.

The following table lists the interactive commands you can use with the virtual machine storage panel.

Table 511: Virtual Machine Storage Panel Interactive Commands

Command	Description
`e`	Expand or roll up storage VSCSI statistics. Allows you to view storage resource utilization statistics broken down by individual VSCSI devices belonging to a group. You are prompted to enter the group ID. The statistics are per VSCSI device.
`r`	Sort by READS/s column.
`w`	Sort by WRITES/s column.
`R`	Sort by MBREAD/s column.
`T`	Sort by MBWRTN/s column.
`N`	Sort first by VMNAME column, and then by VSCSINAME column. It is the default sort order.

Network Panel

The Network panel displays server-wide network utilization statistics.

Statistics are arranged by port for each virtual network device configured. For physical network adapter statistics, see the row in the table that corresponds to the port to which the physical network adapter is connected. For statistics on a virtual network adapter configured in a particular virtual machine, see the row corresponding to the port to which the virtual network adapter is connected.

Table 512: Network Panel Statistics

Column	Description
PORT-ID	Virtual network device port ID.

Column	Description
UPLINK	Y means that the corresponding port is an uplink. N means it is not.
UP	Y means that the corresponding link is up. N means it is not.
SPEED	Link speed in Megabits per second.
FDUPLX	Y means the corresponding link is operating at full duplex. N means it is not.
USED-BY	Virtual network device port user.
DTYP	Virtual network device type. H means HUB and S means switch.
DNAME	Virtual network device name.
PKTTX/s	Number of packets transmitted per second.
PKTRX/s	Number of packets received per second.
MbTX/s	MegaBits transmitted per second.
MbRX/s	MegaBits received per second.
%DRPTX	Percentage of transmit packets dropped.
%DRPRX	Percentage of receive packets dropped.
TEAM-PNIC	Name of the physical NIC used for the team uplink.
PKTTXMUL/s	Number of multicast packets transmitted per second.
PKTRXMUL/s	Number of multicast packets received per second.
PKTTXBRD/s	Number of broadcast packets transmitted per second.
PKTRXBRD/s	Number of broadcast packets received per second.

The following table displays the interactive commands you can use with the network panel.

Table 513: Network Panel Interactive Commands

Command	Description
`T`	Sorts by Mb Tx column.
`R`	Sorts by Mb Rx column.
`t`	Sorts by Packets Tx column.
`r`	Sorts by Packets Rx column.
`N`	Sorts by PORT-ID column. This is the default sort order.
`L`	Changes the displayed length of the DNAME column.

Interrupt Panel

The interrupt panel displays information about the use of interrupt vectors.

Table 514: Interrupt Panel Statistics

Column	Description
VECTOR	Interrupt vector ID.
COUNT/s	Total number of interrupts per second. This value is cumulative of the count for every CPU.

Column	Description
COUNT_x	Interrupts per second on CPU x.
TIME/int	Average processing time per interrupt (in microseconds).
TIME_x	Average processing time per interrupt on CPU x (in microseconds).
DEVICES	Devices that use the interrupt vector. If the interrupt vector is not enabled for the device, its name is enclosed in angle brackets (< and >).

Using Batch Mode

Batch mode allows you to collect and save resource utilization statistics in a file.

After you prepare for batch mode, you can use `esxtop` or `resxtop` in this mode.

Prepare for Batch Mode

To run in batch mode, you must first prepare for batch mode.

1. Run `resxtop` (or `esxtop`) in interactive mode.
2. In each of the panels, select the columns you want.
3. Save this configuration to a file (by default `~/.esxtop50rc`) using the `W` interactive command.

You can now use `resxtop` (or `esxtop`) in batch mode.

Use esxtop or resxtop in Batch Mode

After you have prepared for batch mode, you can use `esxtop` or `resxtop` in this mode.

1. Start `resxtop` (or `esxtop`) to redirect the output to a file.
   For example:
   ```
   esxtop -b > my_file.csv
   ```
   The filename must have a `.csv` extension. The utility does not enforce this, but the post-processing tools require it.
2. Process statistics collected in batch mode using tools such as Microsoft Excel and Perfmon.

In batch mode, `resxtop` (or `esxtop`) does not accept interactive commands. In batch mode, the utility runs until it produces the number of iterations requested (see command-line option `n`, below, for more details), or until you end the process by pressing Ctrl+c.

Batch Mode Command-Line Options

You can use batch mode with command-line options.

Table 515: Command-Line Options in Batch Mode

Option	Description
`a`	Show all statistics. This option overrides configuration file setups and shows all statistics. The configuration file can be the default `~/.esxtop50rc` configuration file or a user-defined configuration file.
`b`	Runs `resxtop` (or `esxtop`) in batch mode.

Option	Description
c *filename*	Load a user-defined configuration file. If the -c option is not used, the default configuration filename is ~/.esxtop41rc. Create your own configuration file, specifying a different filename, using the W single-key interactive command.
d	Specifies the delay between statistics snapshots. The default is five seconds. The minimum is two seconds. If a delay of less than two seconds is specified, the delay is set to two seconds.
n	Number of iterations. resxtop (or esxtop) collects and saves statistics this number of times, and then exits.
server	The name of the remote server host to connect to (required, resxtop only).
vihost	If you connect indirectly (through vCenter Server), this option should contain the name of the ESXi host you connect to. If you connect directly to the ESXi host, this option is not used. **Note:** The host name needs to be the same as what appears in the vSphere Client.
portnumber	The port number to connect to on the remote server. The default port is 443, and unless this is changed on the server, this option is not needed. (resxtop only)
username	The user name to be authenticated when connecting to the remote host. You are prompted by the remote server for a password, as well (resxtop only).

Using Replay Mode

In replay mode, esxtop replays resource utilization statistics collected using vm-support.

After you prepare for replay mode, you can use esxtop in this mode. See the vm-support man page.

In replay mode, esxtop accepts the same set of interactive commands as in interactive mode and runs until no more snapshots are collected by vm-support to be read or until the requested number of iterations are completed.

Prepare for Replay Mode

To run in replay mode, you must prepare for replay mode.

1. Run vm-support in snapshot mode in the ESXi Shell.

   Use the following command.

   ```
   vm-support -S -d duration -I interval
   ```

2. Unzip and untar the resulting tar file so that esxtop can use it in replay mode.

You can now use esxtop in replay mode.

Use esxtop in Replay Mode

You can use esxtop in replay mode.

Replay mode can be run to produce output in the same style as batch mode (see the command-line option b, below).

Note: Batch output from esxtop cannot be played back by resxtop.

Snapshots collected by vm-supported can be replayed by esxtop. However, vm-support output generated by ESXi can be replayed only by esxtop running on the same version of ESXi.

To activate replay mode, enter the following at the command-line prompt.

```
esxtop -R vm-support_dir_path
```

Replay Mode Command-Line Options

You can use replay mode with command-line options.

The following table lists the command-line options available for `esxtop` replay mode.

Table 516: Command-Line Options in Replay Mode

Option	Description
`R`	Path to the vm-support collected snapshot's directory.
`a`	Show all statistics. This option overrides configuration file setups and shows all statistics. The configuration file can be the default `~/.esxtop50rc` configuration file or a user-defined configuration file.
`b`	Runs `esxtop` in Batch mode.
`c` *`filename`*	Load a user-defined configuration file. If the `-c` option is not used, the default configuration filename is ~/.esxtop50rc. Create your own configuration file and specify a different filename using the `W` single-key interactive command.
`d`	Specifies the delay between panel updates. The default is five seconds. The minimum is two seconds. If a delay of less than two seconds is specified, the delay is set to two seconds.
`n`	Number of iterations `esxtop` updates the display this number of times and then exits.

Using the vimtop Plug-In to Monitor the Resource Use of Services

You can use the `vimtop` utility plug-in to monitor vSphere services that run in the vCenter Server.

`vimtop` is a tool similar to `esxtop`, which runs in the environment of the vCenter Server. By using the text-based interface of `vimtop` in the appliance shell, you can view overall information about the vCenter Server, and a list of vSphere services and their resource use.

Monitor Services By Using vimtop in Interactive Mode

You can use the `vimtop` plug-in to monitor services in real time.

The default view of the `vimtop` interactive mode consists of the overview tables and the main table. You can use single-key commands in interactive mode to switch the view from processes to disks or network.

1. From an SSH client application, log in to the vCenter Server shell.
2. Run the `vimtop` command to access the plug-in in interactive mode.

Related Links

Interactive Mode Command-Line Options on page 1727
You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Interactive Mode Single-Key Commands for vimtop on page 1727
When running in interactive mode, `vimtop` recognizes several single-key commands.

Interactive Mode Command-Line Options

You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Table 517: Interactive Mode Command-Line Options

Option	Description
-h	Prints help for the `vimtop` command-line options.
-v	Prints the `vimtop` version number.
-c *filename*	Loads a user-defined `vimtop` configuration file. If the -c option is not used, the default configuration file is `/root/vimtop/vimtop.xml`. You can create your own configuration file, specifying a different filename and path by using the `W` single-key interactive command.
-n *number*	Sets the number of performed iterations before the `vimtop` exits interactive mode. `vimtop` updates the display *number* number of times and exits. The default value is 10000.
-p / -d*seconds*	Sets the update period in seconds.

Related Links

Monitor Services By Using vimtop in Interactive Mode on page 1727
You can use the `vimtop` plug-in to monitor services in real time.

Interactive Mode Single-Key Commands for vimtop on page 1727
When running in interactive mode, `vimtop` recognizes several single-key commands.

Interactive Mode Single-Key Commands for vimtop

When running in interactive mode, `vimtop` recognizes several single-key commands.

All interactive mode panels recognize the commands listed in the following table.

Table 518: Interactive Mode Single-Key Commands

Key Names	Description
h	Show a help menu for the current panel, giving a brief summary of commands, and the status of secure mode.
i	Show or hide the top line view of the overview panel of the `vimtop` plug-in.
t	Show or hide the Tasks section, which displays information in the overview panel about the tasks currently running on the vCenter Server instance.
m	Show or hide the Memory section in the overview panel.
f	Show or hide the CPU section which displays information in the overview panel about all available CPUs.
g	Show or hide the CPUs section which displays information in the overview panel about the top 4 physical CPUs.
spacebar	Immediately refreshes the current pane.
p	Pause the displayed information about the services resource use in the current panels.
r	Refresh the displayed information about the services resource use in the current panels.
s	Set refresh period.
q	Exit the interactive mode of the `vimtop` plug-in.
k	Displays the Disks view of the main panel.
o	Switch the main panel to Network view.

Key Names	Description
Esc	Clear selection or return to the Processes view of the main panel.
Enter	Select a service to view additional details.
n	Show or hide names of the headers in the main panel.
u	Show or hide the measurement units in the headers in the main panel.
left, right arrows	Select columns.
up, down arrows	Select rows.
<,>	Move a selected column.
Delete	Remove selected column.
c	Add a column to the current view of the main panel. Use spacebar to add or remove columns from the displayed list.
a	Sort the selected column in ascending order.
d	Sort the selected column in descending order.
z	Clear the sort order for all columns.
l	Set width for the selected column.
x	Return the column widths to their default values.
+	Expand selected item.
-	Collapse selected item.
w	Write the current setup to a `vimtop` configuration file. The default file name is the one specified by -c option, or `/root/vimtop/vimtop.xml` if the -c option is not used. You can also specify a different file name on the prompt generated by the `w` command.

Related Links

Monitor Services By Using vimtop in Interactive Mode on page 1727

You can use the `vimtop` plug-in to monitor services in real time.

Interactive Mode Command-Line Options on page 1727

You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Monitoring Networked Devices with SNMP and vSphere

Simple Network Management Protocol (SNMP) is commonly used by management programs to monitor a variety of networked devices.

vSphere systems run SNMP agents, which can provide information to a management program in at least one of the following ways:

- In response to a `GET`, `GETBULK`, or `GETNEXT` operation, which is a specific request for information from the management system.
- By sending a notification which is an alert sent by the SNMP agent to notify the management system of a particular event or condition.

Management Information Base (MIB) files define the information that can be provided by managed devices. The MIB files define managed objects, described by object identifiers (OIDs) and variables arranged in a hierarchy.

vCenter Server and ESXi have SNMP agents. The agent provided with each product has different capabilities.

Using SNMP Traps with vCenter Server

The SNMP agent included with vCenter Server can be used to send traps when vCenter Server starts and when an alarm is triggered on vCenter Server. The vCenter Server SNMP agent functions only as a trap emitter and does not support other SNMP operations, such as receiving `GET`, `GETBULK`, and `GETNEXT` requests.

vCenter Server can send SNMPv1 traps to other management applications. You must configure your management server to interpret the SNMP traps sent by vCenter Server.

To use the vCenter Server SNMP traps, configure the SNMP settings on vCenter Server and your management client software to accept the traps from vCenter Server.

The traps sent by vCenter Server are defined in `VMWARE-VC-EVENT-MIB.mib`.

Configure SNMP Settings for vCenter Server

If you plan to use SNMP with vCenter Server, you must use the vSphere Client to configure the SNMP settings.

- Verify that the vSphere Client is connected to a vCenter Server instance.
- Verify that you have the domain name or IP address of the SNMP receiver, the port number of the receiver, and the community string.

1. In the vSphere Client, navigate to a vCenter Server instance.
2. Click the **Configure** tab.
3. Under Settings, click **General**.
4. On the vCenter Server Settings central pane, click **Edit**.
   The **Edit vCenter Server Settings** wizard opens.
5. Click **SNMP receivers** to edit their settings.
6. Enter the following information for the primary receiver of the SNMP traps.

Option	Description
Primary Receiver URL	Enter the domain name or IP address of the receiver of SNMP traps.
Enable receiver	Select the check box to enable the SNMP receiver.
Receiver port	Enter the port number of the receiver to which the SNMP agent sends traps. If the port value is empty, vCenter Server uses port 162 by default.
Community string	Enter the community string that is used for authentication.

7. Optional: Enter information about other SNMP receivers in the **Receiver 2 URL**, **Receiver 3 URL**, and **Receiver 4 URL** options, and select **Enabled**.
8. Click **OK**.

The vCenter Server system is now ready to send traps to the management system you have specified.
Configure your SNMP management software to receive and interpret data from the vCenter Server SNMP agent. See Configure SNMP Management Client Software.

Configure SNMP for ESXi

ESXi includes an SNMP agent that can send notifications (traps and informs) and receive `GET`, `GETBULK`, and `GETNEXT` requests.

In ESXi 5.1 and later releases, the SNMP agent adds support for version 3 of the SNMP protocol, offering increased security and improved functionality, including the ability to send informs. You can use `esxcli` commands to enable and configure the SNMP agent. You configure the agent differently depending on whether you want to use SNMP v1/v2c or SNMP v3.

As an alternative to configuring SNMP manually using `esxcli` commands, you can use host profiles to configure SNMP for an ESXi host. See the *vSphere Host Profiles* documentation for more information.

Note: For information on configuring SNMP for ESXi 5.0 or earlier or ESX 4.1 or earlier, see the documentation for the appropriate product version.

Configure the SNMP Agent for Polling

If you configure the ESXi SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET`, `GETNEXT` and `GETBULK` requests.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

By default, the embedded SNMP agent listens on UDP port 161 for polling requests from management systems. You can use the `esxcli system snmp set` command with the --port option to configure an alternative port. To avoid conflicting with other services, use a UDP port that is not defined in `/etc/services`.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

1. Run the `esxcli system snmp set` command with the --port option to configure the port.
   For example, run the following command:
   ```
   esxcli system snmp set --port port
   ```
   Here, *`port`* is the port the SNMP agent uses to listen for polling requests.

   Note: The port you specify must not be already in use by other services. Use IP addresses from the dynamic range, port 49152 and up.
2. Optional: If the ESXi SNMP agent is not enabled, run the following command:
   ```
   esxcli system snmp set --enable true
   ```

Configure ESXi for SNMPv1 and SNMPv2c

When you configure the ESXi SNMP agent for SNMPv1 and SNMPv2c, the agent supports sending notifications (traps and informs) and receiving `GET`, `GETBULK`, and `GETNEXT` requests.

In SNMPv1 and SNMPv2c, authentication is performed by using community strings. Community strings are namespaces which contain one or more managed objects. This form of authentication does not secure the communication between the SNMP agent and the management system. To secure the SNMP communication in your environment, use SNMPv3.

Configure SNMP Communities

To enable the ESXi SNMP agent to send and receive SNMP v1 and v2c messages, you must configure at least one community for the agent.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

Run the `esxcli system snmp set` command with the --communities option to configure an SNMP community.
For example, to configure public, East, and West network operation centers communities, run the following command:

```
esxcli system snmp set --communities public,eastnoc,westnoc
```

Each time you specify a community with this command, the settings you specify overwrite the previous configuration. To specify multiple communities, separate the community names with a comma.

Configure the SNMP Agent to Send SNMP v1 or v2c Notifications

You can use the ESXi SNMP agent to send virtual machine and environmental notifications to management systems.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

To send SNMP v1/v2c notifications with the SNMP agent, you must configure the target (receiver) unicast address, community, and an optional port. If you do not specify a port, the SNMP agent sends traps to UDP port 162 on the target management system by default.

To configure SNMP v3 traps, see Configure SNMP v3 Targets.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

1. Run the `esxcli system snmp set` command with the --targets option:

   ```
   esxcli system snmp set --targets target_address@port/community
   ```

   Here, *`target_address`* is the address of the target system, *`port`* is the port number to send the notifications to, and *`community`* is the community name.

   Each time you specify a target with this command, the settings you specify overwrite all previously specified settings. To specify multiple targets, separate them with a comma.

   For example, run the following command for configuring the targets 192.0.2.1@163/westnoc and 2001:db8::1@163/eastnoc:

   ```
   esxcli system snmp set --targets 192.0.2.1@163/westnoc,2001:db8::1@163/eastnoc
   ```

2. Optional: If the ESXi SNMP agent is not enabled, run the following command:

   ```
   esxcli system snmp set --enable true
   ```

3. Optional: Send a test trap to verify that the agent is configured correctly by running the `esxcli system snmp test` command.

   The agent sends a `warmStart` trap to the configured target.

Configure ESXi for SNMP v3

When you configure the ESXi SNMP agent for SNMPv3, the agent supports sending notifications (traps and informs) and receiving `GET`, `GETBULK`, and `GETNEXT` requests. SNMPv3 also provides stronger security than SNMPv1 or SNMPv2c, including key authentication and encryption.

Inform is a notification that the sender resends up to three times or until the receiver acknowledges the notification.

Configure the SNMP Engine ID

Every SNMP v3 agent has an engine ID which serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

If you do not specify an engine ID, when you enable the SNMP agent, an engine ID is automatically generated.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

Run the `esxcli system snmp set` command with the --engineid option to configure the SNMP engine ID.
For example, run the following command:

```
esxcli system snmp set --engineid id
```

Here, *`id`* is the engine ID and it must be a hexadecimal string between 5 and 32 characters long.

Configure SNMP Authentication and Privacy Protocols

SNMPv3 optionally supports authentication and privacy protocols.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

Authentication is used to ensure the identity of users. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data. These protocols provide a higher level of security than is available in SNMPv1 and SNMPv2c, which use community strings for security.

Both authentication and privacy are optional. However, you must enable authentication to enable privacy.

The SNMPv3 authentication and privacy protocols are licensed vSphere features and might not be available in some vSphere editions.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

1. Optional: Run the `esxcli system snmp set` command with the --authentication option to configure authentication.
   For example, run the following command:

   ```
   esxcli system snmp set --authentication protocol
   ```

   Here, *`protocol`* must be either `none` (for no authentication) or `SHA1`.
2. Optional: Run the `esxcli system snmp set` command with the --privacy option to configure privacy.
   For example, run the following command:

   ```
   esxcli system snmp set --privacy protocol
   ```

   Here, *`protocol`* must be either `none` (for no privacy) or `AES128`.

Configure SNMP Users

You can configure up to 5 users who can access SNMP v3 information. User names must be no more than 32 characters long.

- Verify that you have configured the authentication and privacy protocols before configuring users.
- Verify that you know the authentication and privacy passwords for each user you plan to configure. Passwords must be at least 7 characters long. Store these passwords in files on the host system.
- Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

While configuring a user, you generate authentication and privacy hash values based on the user's authentication and privacy passwords and the SNMP agent's engine ID. If you change the engine ID, the authentication protocol, or the privacy protocol after configuring users, the users are no longer valid and must be reconfigured.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

1. If you are using authentication or privacy, get the authentication and privacy hash values for the user by running the `esxcli system snmp hash` command with the --auth-hash and --priv-hash flags.
   For example, run the following command:
   ```
   esxcli system snmp hash --auth-hash secret1 --priv-hash secret2
   ```
   Here, *`secret1`* is the path to the file containing the user's authentication password and *`secret2`* is the path to the file containing the user's privacy password.

   Alternatively, you can pass the --raw-secret flag and specify the passwords directly on the command line.

   For example, you can run the following command:
   ```
   esxcli system snmp hash --auth-hash authsecret --priv-hash privsecret --raw-secret
   ```
   The produced output might be the following:
   ```
   Authhash: 08248c6eb8b333e75a29ca0af06b224faa7d22d6
   Privhash: 232ba5cbe8c55b8f979455d3c9ca8b48812adb97
   ```
   The authentication and privacy hash values are displayed.
2. Configure the user by running the `esxcli system snmp set` command with the --user flag.
   For example, you can run the following command:
   ```
   esxcli system snmp set --users userid/authhash/privhash/security
   ```
   The command accepts the following parameters:

Parameter	Description
`userid`	The user name.
`authhash`	The authentication hash value.
`privhash`	The privacy hash value.
`security`	The level of security enabled for that user, which can be *`auth`* (for authentication only), *`priv`* (for authentication and privacy), or *`none`* (for no authentication or privacy).

   For example, run the following command to configure user1 for access with authentication and privacy:
   ```
   esxcli system snmp set --users user1/08248c6eb8b333e75a29ca0af06b224faa7d22d6/
   ```

```
232ba5cbe8c55b8f979455d3c9ca8b48812adb97/priv
```

You must run the following command to configure user2 for access with no authentication or privacy:

```
esxcli system snmp set --users user2/-/-/none
```

3. Optional: Test the user configuration by running the following command:

   ```
   esxcli system snmp test --user username--auth-hash secret1--priv-hash secret2
   ```

   If the configuration is correct, this command returns the following message: "User *username* validated correctly using engine id and security level: *protocols*". Here, *protocols* indicates the security protocols configured.

Configure SNMP v3 Targets

Configure SNMP v3 targets to allow the ESXi SNMP agent to send SNMP v3 traps and informs.

- Ensure that the users who access the traps or informs are configured as SNMP users for both the ESXi SNMP agent and the target management system.
- If you are configuring informs, you need the engine ID for the SNMP agent on the remote system that receives the inform message.
- Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

SNMP v3 allows for sending both traps and informs. An inform message is a type of a message that the sender resends a maximum of three times. The sender waits for 5 seconds between each attempt, unless the message is acknowledged by the receiver.

You can configure a maximum of three SNMP v3 targets, in addition to a maximum of three SNMP v1/v2c targets.

To configure a target, you must specify a hostname or IP address of the system that receives the traps or informs, a user name, a security level, and whether to send traps or informs. The security level can be either `none` (for no security), `auth` (for authentication only), or `priv` (for authentication and privacy).

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

1. Optional: If you are configuring informs, configure the remote users by running the `esxcli system snmp set` command with the --remote-users option.
   For example, run the following command:

   ```
   esxcli system snmp set --remote-users userid/auth-protocol/auth-hash/priv-protocol/priv-hash/engine-id
   ```

   The command accepts the following parameters:

Parameter	Description
userid	The user name.
auth-protocol	The authentication protocol, `none` (for no authentication) or `SHA1`.
auth-hash	The authentication hash or − if the authentication protocol is `none`.
priv-protocol	The privacy protocol, `AES128`, or `none`.
priv-hash	The privacy hash, or − if the privacy protocol is `none`.
engine-id	The engine ID of the SNMP agent on the remote system that receives the inform message.

2. Run the `esxcli system snmp set` command with the --v3targets option.
   For example, run the following command:
   ```
   esxcli system snmp set --v3targets hostname@port/userid/secLevel/message-type
   ```
   The parameters of the command are as follows.

Parameter	Description
hostname	The host name or IP address of the management system that receives the traps or informs.
port	The port on the management system that receives the traps or informs. If you do not specify a port, the default port, 162, is used.
userid	The user name.
secLevel	The level of authentication and privacy you have configured. Use `auth` if you have configured authentication only, `priv` if you have configured both authentication and privacy, and `none` if you have configured neither.
message-type	The type of the messages received by the management system. Use `trap` or `inform`.

3. Optional: If the ESXi SNMP agent is not enabled, run the following command:
   ```
   esxcli system snmp set --enable true
   ```
4. Optional: Send a test notification to verify that the agent is configured correctly by running the `esxcli system snmp test` command.
   The agent sends a `warmStart` notification to the configured target.

Configure the Source of Hardware Events Received by the SNMP Agent

You can configure the ESXi SNMP agent to receive hardware events either from IPMI sensors or CIM indications.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

IPMI sensors are used for hardware monitoring in ESX/ESXi 4.x and earlier. The conversion of CIM indications to SNMP notifications is available in ESXi 5.0 and later.

If you run ESXCLI commands through ESXCLI, you must supply connection options that specify the target host and login credentials. If you use ESXCLI commands directly on a host using the ESXi Shell, you can use the commands as given without specifying connection options. For more information on connection options see *ESXCLI Concepts and Examples*.

1. Run the `esxcli system snmp set --hwsrc source` command to configure the source for hardware events.
   Here, *source* is `sensors` or `indications`, for hardware event received from IPMI sensors or CIM indications respectively.
2. Optional: If the ESXi SNMP agent is not enabled, run the following command:
   ```
   esxcli system snmp set --enable true
   ```

Configure the SNMP Agent to Filter Notifications

You can configure the ESXi SNMP agent to filter out notifications if you don't want your SNMP management software to receive those notifications.

Configure the ESXi SNMP agent by using the ESXCLI commands. See *Getting Started with ESXCLI* for more information on how to use ESXCLI.

1. Run the `esxcli system snmp set` command to filter notifications:

   ```
   esxcli system snmp set --notraps oid_list
   ```

   Here, *`oid_list`* is a list of OIDs for the notifications to filter, separated by commas. This list replaces any OIDs that were previously specified using this command.

   For example, to filter out `coldStart` (OID `1.3.6.1.4.1.6876.4.1.1.0`) and `warmStart` (OID `1.3.6.1.4.1.6876.4.1.1.1`) traps, run the following command:

   ```
   esxcli system snmp set --notraps 1.3.6.1.4.1.6876.4.1.1.0,1.3.6.1.4.1.6876.4.1.1.1
   ```

2. Optional: If the ESXi SNMP agent is not enabled, run the following command:

   ```
   esxcli system snmp set --enable true
   ```

The traps identified by the specified OIDs are filtered out of the output of the SNMP agent, and are not sent to SNMP management software.

To clear all notification filters, run the `esxcli system snmp set --notraps reset` command.

Configure SNMP Management Client Software

After you have configured a vCenter Server instance or an ESXi host to send traps, configure your management client software to receive and interpret those traps.

To complete this task, download the VMware MIB files from https://kb.vmware.com/s/article/1013445.

To configure your management client software, specify the communities for the managed device, configure the port settings, and load the VMware MIB files. See the documentation for your management system for specific instructions for these steps.

1. In your management software, specify the vCenter Server instance or ESXi host as an SNMP-based managed device.
2. If you are using SNMPv1 or SNMPv2c, set up appropriate community names in the management software.

   These names must correspond to the communities set for the SNMP agent on the vCenter Server instance or ESXi host.
3. If you are using SNMPv3, configure users and authentication and privacy protocols to match those configured on the ESXi host.
4. If you configured the SNMP agent to send traps to a port on the management system other than the default UDP port 162, configure the management client software to listen on the port you configured.
5. Load the VMware MIBs into the management software so you can view the symbolic names for vCenter Server or the host variables.

   To prevent lookup errors, load these MIB files in the following order before loading other MIB files:

   1. `VMWARE-ROOT-MIB.mib`
   2. `VMWARE-TC-MIB.mib`
   3. `VMWARE-PRODUCTS-MIB.mib`

The management software can now receive and interpret traps from vCenter Server or ESXi hosts.

SNMP Diagnostics

You can use SNMP tools to diagnose configuration problems.

- Run the `esxcli system snmp test` command from the ESXCLI set to prompt the SNMP agent to send a test `warmStart` trap.

- Run the `esxcli system snmp get` command to display the current configuration of the SNMP agent.
- The `SNMPv2-MIB.mib` file provides several counters to aid in debugging SNMP problems. See SNMPv2 Diagnostic Counters.
- The `VMWARE-ESX-AGENTCAP-MIB.mib` file defines the capabilities of the VMware SNMP agents by product version. Use this file to determine if the SNMP functionality that you want to use is supported.

Monitor Guest Operating Systems with SNMP

You can use SNMP to monitor guest operating systems or applications running in virtual machines.

The virtual machine uses its own virtual hardware devices. Do not install agents in the virtual machines that are intended to monitor physical hardware.

- Install the SNMP agents you normally would use for that purpose in the guest operating systems.

VMware MIB Files

VMware MIB files contain information provided by ESXi hosts and vCenter Server to SNMP management software.

Management Information Base (MIB) files define the information that can be provided by managed devices. The MIB files define managed objects, described by object identifiers (OIDs) and variables arranged in a hierarchy. SMI structure of management information (RFC 2578) is the syntax used to write MIB files for specific product and function. These MIB files are versioned independently of product and can be used to identify event types and event data related information.

You can download these MIB files from https://kb.vmware.com/s/article/1013445.

Table 1. VMware MIB Files lists the MIB files provided by VMware and describes the information provided by each file.

Table 519: VMware MIB Files

MIB File	Description
`VMWARE-ROOT-MIB.mib`	Contains VMware's enterprise OID and top-level OID assignments.
`VMWARE-ESX-AGENTCAP-MIB.mib`	Defines the capabilities of the VMware agents by product versions. This file is optional and might not be supported by all management systems.
`VMWARE-CIMOM-MIB.mib`	Defines variables and trap types used to report on the state of the CIM Object Management subsystem.
`VMWARE-ENV-MIB.mib`	Defines variables and trap types used to report on the state of physical hardware components of the host computer. Enables conversion of CIM indications to SNMP traps.
`VMWARE-OBSOLETE-MIB.mib`	For use with versions of ESX/ESXi prior to 4.0. Defines OIDs that have been made obsolete to maintain backward compatibility with earlier versions of ESX/ESXi. Includes variables formerly defined in the files VMWARE-TRAPS-MIB.mib and VMWARE-VMKERNEL-MIB.mib.
`VMWARE-PRODUCTS-MIB.mib`	Defines OIDs to uniquely identify each SNMP agent on each VMware platform by name, version, and build platform.
`VMWARE-RESOURCES-MIB.mib`	Defines variables used to report information on resource usage of the VMkernel, including physical memory, CPU, and disk utilization.
`VMWARE-SYSTEM-MIB.mib`	The `VMWARE-SYSTEM-MIB.mib` file is obsolete. Use the SNMPv2-MIB to obtain information from `sysDescr.0` and `sysObjec ID.0`.
`VMWARE-TC-MIB.mib`	Defines common textual conventions used by VMware MIB files.
`VMWARE-VC-EVENT-MIB.mib`	Defines traps sent by vCenter Server. Load this file if you use vCenter Server to send traps.

MIB File	Description
VMWARE-VMINFO-MIB.mib	Defines variables for reporting information about virtual machines, including virtual machine traps.

Table 2. Other MIB Files lists MIB files included in the VMware MIB files package that are not created by VMware. These can be used with the VMware MIB files to provide additional information.

Table 520: Other MIB Files

MIB File	Description
ENTITY-MIB.mib	Allows the description of relationships between physical entities and logical entities managed by the same SNMP agent. See RFC 4133 for more information.
HOST-RESOURCES-MIB.mib	Defines objects that are useful for managing host computers.
HOST-RESOURCES-TYPES.mib	Defines storage, device, and filesystem types for use with HOST-RESOURCES-MIB.mib.
IEEE8021-BRIDGE-MIB	Defines objects for managing devices that support IEEE 802.1D.
IEEE8023-LAG-MIB	Defines objects for managing devices that support IEEE 802.3ad link aggregation.
IEEE8021-Q-BRIDGE-MIB	Defines objects for managing Virtual Bridged Local Area Networks.
IF-MIB.mib	Defines attributes related to physical NICs on the host system.
IP-MIB.mib	Defines objects for managing implementations of the Internet Protocol (IP) in an IP version-independent manner.
IP-FORWARD-MIB.mib	Defines objects for managing IP forwarding.
LLDP-V2-MIB.mib	Defines objects for managing devices using Linked Layer Discovery Protocol (LLDP).
SNMPv2-CONF.mib	Defines conformance groups for MIBs.
SNMPv2-MIB.mib	Defines the SNMP version 2 MIB objects.
SNMPv2-SMI.mib	Defines the Structure of Management Information for SNMP version 2.
SNMPv2-TC.mib	Defines textual conventions for SNMP version 2.
TCP-MIB.mib	Defines objects for managing devices using the TCP protocol.
UDP-MIB.mib	Defines objects for managing devices using the UDP protocol.

SNMPv2 Diagnostic Counters

The SNMPv2-MIB.mib file provides a number of counters to aid in debugging SNMP problems.

Table 521: Diagnostic Counters from SNMPv2-MIB lists some of these diagnostic counters.

Table 521: Diagnostic Counters from SNMPv2-MIB

Variable	ID Mapping	Description
snmpInPkts	snmp 1	The total number of messages delivered to the SNMP entity from the transport service.

Variable	ID Mapping	Description
snmpInBadVersions	snmp 3	The total number of SNMP messages that were delivered to the SNMP entity and were for an unsupported SNMP version.
snmpInBadCommunityNames	snmp 4	The total number of community-based SNMP messages delivered to the SNMP entity that used an invalid SNMP community name.
snmpInBadCommunityUses	snmp 5	The total number of community-based SNMP messages delivered to the SNMP entity that represented an SNMP operation that was not allowed for the community named in the message.
snmpInASNParseErrs	snmp 6	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpEnableAuthenTraps	snmp 30	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information. It therefore provides a means of disabling all authenticationFailure traps.
snmpSilentDrops	snmp 31	The total number of Confirmed Class PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate Response Class PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	snmp 32	The total number of Confirmed Class PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in a manner other than a time-out such that no Response Class PDU could be returned.

System Log Files

In addition to lists of events and alarms, vSphere components generate assorted logs.

These logs contain additional information about activities in your vSphere environment.

View System Logs on an ESXi Host

You can use the Direct Console User Interface (DCUI) to view system logs on an ESXi host. These logs provide information about system operational events.

1. From the ESXi Host Client, click **Manage** > **Services**. Confirm that the DCUI service is running.
2. Open an SSH client (such as PuTTY) and connect to the ESXi host.
3. Log in with the root account.
4. Enter `DCUI` to start the Direct Console User Interface.
5. Click inside the console window and press F2 to customize the system.
6. Type the password for the root user and press Enter.
7. Use the arrow keys to select **View System Logs**.
8. Press a corresponding number key to view a log.
   vCenter Server agent (vpxa) logs appear if the host is managed by vCenter Server.
9. Press Enter or the spacebar to scroll through the messages.
10. Optional: Perform a regular expression search.
    a) Press the slash key (/).
    b) Type the text to find.
    c) Press Enter
       The found text is highlighted on the screen.
11. Press q to return to the direct console.

System Logs

VMware technical support might request several files to help resolve any issues you might have with the product. This section describes the types and locations of log files found on ESXi hosts and vSphere Client.

ESXi System Logs

You might need the ESXi system log files to resolve technical issues.

The ESXi system logs can be found in the `/var/run/log` directory.

vSphere Client Logs

You might need the vSphere Client system log files to resolve technical issues.

When you use a vCenter Server instance, the vSphere Client system logs can be found in the location listed in the table.

Table 522: Location of vSphere Client Logs

vCenter Server System	Location
vCenter Server	`/var/log/vmware/vsphere-ui/logs`

The main vSphere Client log file is `vsphere_client_virgo.log`.

Export System Log Files

When the vSphere Client is connected to vCenter Server, you can select hosts from which to download system log files.

To save diagnostic data for ESXi hosts and vCenter Server, the vSphere Clientmust be connected to the vCenter Server system.

Required privileges:

- To view diagnostic data: **Read-Only User**
- To manage diagnostic data: **Global** > **Diagnostics**

1. In the inventory, right click a vCenter Server instance.
   Export System Logs option is available for Hosts and Virtual Machines.
2. Click **Export System Logs**.
3. If you are connected to vCenter Server, select the object for which you want to export data.
   Selecting an object selects all of its child objects.
4. If you are connected to vCenter Server, select **Include information from vCenter Server and vSphere UI logs** to download vCenter Server and vSphere Client log files and host log files, and click **Next**.
5. If the selected host supports manifest driven exports of system log files, select the system log files to collect. Select the specific system log files to download.
   If the host does not support manifest exports of log files, all system log files are exported.
6. Select **Gather performance data** to include performance data information in the log files.
   You can update the duration and interval time you want the data collected.
7. Optional: Select to apply a password for encrypted core dumps to the support package.
   You can make that password available to your support representative in a secure channel.
   If only some of the host in your environment use encryption, some of the files in the package are encrypted.
8. Click **Finish**.
9. Specify the location to which to save the log files.
   The host or vCenter Server generates a `.zip` file containing the log files.
   The **Recent Tasks** panel shows the Generate diagnostic bundles task in progress.
   The Downloading Log Bundles dialog box appears when the Generating Diagnostic Bundle task is finished. The download status of each bundle appears in the dialog box.
   Some network errors can cause download failures. When you select an individual download in the dialog box, the error message for that operation appears under the name and location of the log bundle file.
10. Click **Save**.
11. Verify the information in the Summary and click **Finish** to download the log files.

Diagnostic bundles containing log files for the specified objects are downloaded to the location specified.

Upload Logs Package to a VMware Service Request.

ESXi Log Files

Log files are an important component of troubleshooting attacks and obtaining information about breaches. Logging to a secure, centralized log server can help prevent log tampering. Remote logging also provides a long-term audit record.

To increase the security of the host, take the following measures.

- Configure persistent logging to a datastore. By default, the logs on ESXi hosts are stored in the in-memory file system. Therefore, they are lost when you reboot the host, and only 24 hours of log data is stored. When you enable persistent logging, you have a dedicated activity record for the host.
- Remote logging to a central host allows you to gather log files on a central host. From that host, you can monitor all hosts with a single tool, do aggregate analysis, and search log data. This approach facilitates monitoring and reveals information about coordinated attacks on multiple hosts.
- Configure the remote secure syslog on ESXi hosts by using ESXCLI or PowerCLI, or by using an API client.
- Query the syslog configuration to make sure that the syslog server and port are valid.

See the *vSphere Monitoring and Performance* documentation for information about syslog setup, and for additional information on ESXi log files.

Upload Logs Package to a VMware Service Request

If you already have a Service Request ID with VMware, you can use the vSphere Client to upload the system log bundles directly to your service request.

Request a Service Request ID from VMware Technical Support.

1. In the vSphere Client, navigate to **Administration**.
2. Click **Support**, and click **Upload File to Service Request**.
   An Upload File to Service Request dialog box opens.
3. Enter your Service Request ID with VMware.
4. Click **Choose File**, and select the log bundle you want to attach to your service request with VMware, and click **OK**.
5. If you protected your support package with a password, provide the password to VMware Technical Support by using a secure channel.

The log bundle is sent to your service request.

Configure Syslog on ESXi Hosts

You can use the vSphere Client, the VMware Host Client, or the `esxcli system syslog` command to configure the syslog service.

The syslog service receives, categorizes, and stores log messages for analyses that help you take preventive action in your environment.

Configuring Logging Levels for the Guest Operating System

Virtual machines can write support and troubleshooting information into a virtual machine log file stored on a VMFS volume. The default settings for virtual machines are appropriate for most situations.

If your environment relies heavily on using vMotion, or if the defaults do not seem suitable for other reasons, you can modify the logging settings for virtual machine guest operating systems.

New log file creation happens as follows:

- Each time you power on or resume a virtual machine, and each time you migrate a virtual machine with vMotion, a new log file is created.
- Each time an entry is written to the log, the size of the log is checked. If `vmx.log.rotateSize` is set to a nondefault value, and the size is over the limit, the next entry is written to a new log. If the maximum number of log files exists, the oldest log file is deleted.

The default for vmx.log.rotateSize is zero (0), which means new logs are created during power-on, resume, and so on. You can ensure the new log file creation happens more frequently by limiting the maximum size of the log files with the vmx.log.rotateSize configuration parameter.

VMware recommends saving 10-log files, each one limited to no less than 2MB. These values are large enough to capture sufficient information to debug most problems. If you need logs for a longer time span, you can set vmx.log.keepOld to 20.

Change the Number of Virtual Machine Log Files

You can change the number of the log files for all virtual machines on an ESXi host or for individual virtual machines.

Turn off the virtual machine.

This procedure discusses limiting the virtual machine log file number on an individual virtual machine.

To limit the number of log files for *all* virtual machines on a host, edit the /etc/vmware/config file. If the vmx.log.KeepOld property is not defined in the file, you can add it. For example, to keep ten log files for each virtual machine, add the following to /etc/vmware/config:

```
vmx.log.keepOld = "10"
```

You can use a PowerCLI script to change this property on all the virtual machines on a host.

You can use the log.keepOld parameter to affect all log files, not just the virtual machine log files.

1. Log in to a vCenter Server system using the vSphere Client and find the virtual machine.
   a) In the Navigator, select **VMs and Templates**.
   b) Find the virtual machine in the hierarchy.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Add or edit the vmx.log.keepOld parameter to the number of files to keep for this virtual machine.
   For example, to keep 20 log files and begin deleting the oldest files as new ones are created, enter 20.
6. Click **OK**.

Control When to Switch to New Virtual Machine Log Files

The vmx.log.rotateSize parameter specifies the log file size at which the switch to new log files happens for the logs for individual virtual machines. Use this parameter together with the vmx.log.keepOld parameter to ensure acceptable log file sizes without losing critical logging information.

Turn off the virtual machine.

The vmx.log.keepOld parameter determines how many virtual machine log file instances the ESXi host retains before overwriting the first log file. The default value of vmx.log.keepOld is 10, a suitable number to properly log complex operations such as vMotion. You must increase this number significantly when you change the value of vmx.log.rotateSize.

This procedure discusses changing the virtual machine rotate size on an individual virtual machine.

To limit the rotate size for *all* virtual machines on a host, edit the /etc/vmware/config file. If the vmx.log.KeepOld property is not defined in the file, you can add it. You can use a PowerCLI script to change this parameter for selected virtual machines on a host.

You can use the log.rotateSize parameter to affect all log files, not just the virtual machine log files.

You can change the value of `vmx.log.rotateSize` for all virtual machines from the vSphere Client or by using a PowerCLI script.

1. Log in to a vCenter Server system using the vSphere Client and find the virtual machine.
   a) In the Navigator, select **VMs and Templates**.
   b) Find the virtual machine in the hierarchy.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Add or edit the `vmx.log.rotateSize` parameter to the maximum file size before log information is added to a new file.

   Alternatively, you can add or edit the first log file if you have more log files than the `vmx.log.keepOld` parameter specifies.

   Specify the size in bytes.
6. Click **OK**.

Collecting Log Files

VMware technical support might request several files to help resolve technical issues. The following sections describe script processes for generating and collecting some of these files.

Set Verbose Logging

You can set the verbose log file specification

You can set verbose logging for vpxd logs.

1. Select a vCenter Server instance.
2. Click **Configure** tab.
3. Click **General** and in the vCenter Server Settings, click **EDIT**.
4. In the Edit vCenter general settings window, Click **Logging Settings** and select **verbose** from the Log level drop down menu.
5. Click **SAVE**.

Collect vSphere Log Files

You can collect vSphere log files in to a single location.

You can download the log bundle from vSphere Client connected to a vCenter Server system.

1. In vSphere Client menu, select **Administration** > **Deployment** > **System Configuration**.
2. Select a vCenter Server node and click **Export Support Bundle**.
3. Select the support bundle type:
   - Full Support Bundle: Contains information on all services.
   - Minimal Support Bundle: Contains basic product and configuration information.
   - Custom Support Bundle: Contains customized information. Select any of the manifest properties to download the corresponding log files.

4. Click **EXPORT**.
5. Optional: You can also download the vCenter log bundle using another method:
   1. Right click vCenter Server instance and click **Actions** > **Export System Logs...**.
   2. Click **Select hosts** to put selected host logs into an export bundle. Check **Include vCenter Server and vSphere UI Client logs** to optionally include vCenter Server and vSphere UI logs in the bundle. Click **NEXT**.
   3. Click **Select logs** to select specific system logs to export. Click **EXPORT LOGS**.

   Note: The log bundle is generated as a `.zip` file. By default, the vpxd logs within the bundle are compressed as `.tgz` files. You must use `gunzip` to uncompress these files.

Collect ESXi Log Files

You can collect and package all relevant ESXi system and configuration information, a well as ESXi log files. This information can be used to analyze the problems.

- Run the following script on the ESXi Shell: `/usr/bin/vm-support`
  The resulting file has the following format: `esx-`*`date`*`-`*`unique`*`-`*`xnumber`*`.tgz`

ESXi Log File Locations

ESXi records host activity in log files, using a syslog facility.

Table 523: ESXi Log File Locations

Component	Location	Purpose
Authentication	`/var/log/auth.log`	Contains all events related to authentication for the local system.
ESXi host agent log	`/var/log/hostd.log`	Contains information about the agent that manages and configures the ESXi host and its virtual machines.
Shell log	`/var/log/shell.log`	Contains a record of all commands typed into the ESXi Shell and shell events (for example, when the shell was enabled).
System messages	`/var/log/syslog.log`	Contains all general log messages and can be used for troubleshooting. This information was formerly located in the messages log file.
vCenter Server agent log	`/var/log/vpxa.log`	Contains information about the agent that communicates with vCenter Server (if the host is managed by vCenter Server).
Virtual machines	The same directory as the affected virtual machine's configuration files, named `vmware.log` and `vmware*.log`. For example, `/vmfs/volumes/datastore/virtual machine/vmware.log`	Contains virtual machine power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, machine clones, and so on.
VMkernel	`/var/log/vmkernel.log`	Records activities related to virtual machines and ESXi.
VMkernel summary	`/var/log/vmksummary.log`	Used to determine uptime and availability statistics for ESXi (comma separated).

Component	Location	Purpose
VMkernel warnings	`/var/log/vmkwarning.log`	Records activities related to virtual machines.
Quick Boot	`/var/log/loadESX.log`	Contains all events related to restarting an ESXi host through Quick Boot.
Trusted infrastructure agent	`/var/run/log/kmxa.log`	Records activities related to the Client Service on the ESXi Trusted Host.
Key Provider Service	`/var/run/log/kmxd.log`	Records activities related to the vSphere Trust Authority Key Provider Service.
Attestation Service	`/var/run/log/attestd.log`	Records activities related to the vSphere Trust Authority Attestation Service.
ESX Token Service	`/var/run/log/esxtokend.log`	Records activities related to the vSphere Trust Authority ESX Token Service.
ESX API Forwarder	`/var/run/log/esxapiadapter.log`	Records activities related to the vSphere Trust Authority API forwarder.

Configure Log Filtering on ESXi Hosts

The log filtering capability lets you modify the logging policy of the syslog service that is running on an ESXi host.

You can create log filters to reduce the number of repetitive entries in the ESXi logs and to denylist specific log events entirely.

Install ESXCLI. See *Getting Started with ESXCLI*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

Starting with vSphere 7.0 Update 2, you can add log filters and enable log filtering by using ESXCLI. A log filter, once established, remains in place until it is removed, even across ESXi reboots.

Log filters affect all log events that are processed by the ESXi host `vmsyslogd` service, whether they are recorded to a log directory or to a remote syslog server.

You must enable the log filtering capability and reload the syslog daemon to activate the log filters on the ESXi host.

ESXCLI commands to configure log filters follow this pattern: `esxcli system syslog config logfilter {cmd} [cmd options]`.

For example, to get the list of available log filters, run the following command: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter list`.

Use the `set` command to activate or deactivate log filtering: `[root@xxx-xx-dhcp-xx-xx:~] esxcli system syslog config logfilter set`.

Use the `add` command to add a log filter and the `remove` command to remove a log filter.

Use the `get` command to determine if log filtering is enabled.

A log filter is specified by three components and uses the following syntax: `numLogs | ident | logRegexp`.

Parameter	Description
`numLogs`	Specifies the number of matches of the logRegexp Python regular expression that will be allowed before filtering begins.

Parameter	Description
`ident`	The `ident` string is how an application identifies itself to the syslog facility. The `logRegexp` filter must be associated with the same application. You can find the `ident` string of an application by inspecting the log files in `/var/run/log`. The third field of each log file begins with the `ident` string and ends with `[`.
`logRegexp`	Python regular expression that identifies the messages which you want to filter out.

For example, to filter out all messages from the hostd daemon that contain the word "mark" after the tenth occurrence, use the following command: `esxcli system syslog config logfilter add --filter="10|Hostd|mark"`.

To remove the log filter, use the command `esxcli system syslog config logfilter remove --filter="10|Hostd|mark"`.

For more information, see ESXi Syslog Options.

Turn Off Compression for vpxd Log Files

By default, vCenter Server`vpxd` log files are rolled up and compressed into `.gz` files. You can turn off this setting to leave the `vpxd` logs uncompressed.

1. Log in to the vCenter Server using the vSphere Client.
2. Select **Administration** > **vCenter Server Settings**.
3. Select **Advanced Settings**.
4. In the **Key** text box, type `log.compressOnRoll`.
5. In the **Value** text box, type `false`.
6. Click **Add**, and click **OK**.

ESXi VMkernel Files

If the VMkernel fails, an error message appears and then the virtual machine reboots. If you specified a VMware core dump partition when you configured your virtual machine, the VMkernel also generates a core dump and error log.

More serious problems in the VMkernel can freeze the machine without an error message or core dump.

vSphere Single Host Management - VMware Host Client

vSphere Single Host Management - VMware Host Client provides information about managing single hosts with the VMware Host Client.

The VMware Host Client can be used to conduct emergency management when vCenter Server is unavailable. You can use the VMware Host Client to perform administrative tasks, basic troubleshooting tasks, and advanced administrative tasks.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we have updated this guide to remove instances of non-inclusive language.

Intended Audience

This information is intended for anyone who wants to use the VMware Host Client to manage single ESXi hosts. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

Updated Information

This *vSphere Single Host Management - VMware Host Client* is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Single Host Management - VMware Host Client*.

Revision	Description
21 OCT 2022	Minor updates in Configure Userworld Memory Zeroing.
19 OCT 2022	Minor updates in Enable or Disable Virtualization-based Security on an Existing VM in the VMware Host Client.
13 OCT 2022	Removed the blank spaces in the code snippets in Unable to Connect from the VMware Host Client to an ESXi Host After Upgrading to a Newer Version of ESXi.
29 JULY 2022	• Updated theESXi password requirements in Configure the Passwords and Account Lockout Policy in the VMware Host Client. • Updated the step 3 of the procedure in Configure the SOAP Session Timeout in the VMware Host Client.
26 MAY 2022	Updated information in Change Autostart Configuration in theVMware Host Client.
16 MAY 2022	Added a screenshot in Generate a Support Bundle in the VMware Host Client.
12 APR 2022	Added a screenshot in Use Virtual Machine Column Configuration in the VMware Host Client to display the column configuration.
28 OCT 2021	• Consolidated all topics that contain information on how to create a virtual machine in Create a Virtual Machine in the VMware Host Client. • Consolidated all topics that contain information on how to deploy a virtual machine from OVF or OVA file in Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client.

Revision	Description
	• Consolidated all topics that contain information on how to register an existing virtual machine in Register an Existing Virtual Machine in the VMware Host Client. • Minor update to Add an ESXi User in the VMware Host Client. • Minor update to Edit the Time Configuration of anESXi Host in theVMware Host Client. • Updated Unable to Connect from the VMware Host Client to an ESXi Host After Upgrading to a Newer Version of ESXi and removed the outdated version information. • Updated the Maximum Virtual Machine Memory table in Change the Memory Configuration. • Minor update to Change the Number of Virtual CPUs. • Updated diagrams in Setting Up Network for iSCSI and iSER and Best Practices for Configuring Networking with Software iSCSI.
05 OCT 2021	Initial release.

VMware Host Client Overview

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts.

You can use the VMware Host Client to perform administrative and basic troubleshooting tasks, and advanced administrative tasks on your target ESXi host. You can also use the VMware Host Client to conduct an emergency management when vCenter Server is not available.

It is important to know that the VMware Host Client is different from the vSphere Client. You use the vSphere Client to connect to vCenter Server and manage multiple ESXi hosts, whereas you use the VMware Host Client to manage a single ESXi host.

VMware Host Client functions include, but are not limited to the following operations:

- Basic virtualization operations, such as deploying and configuring virtual machines of various complexity
- Creating and managing networking and datastores
- Advanced tuning of host level options to improve performance

VMware Host Client System Requirements

Make sure that your browser supports the VMware Host Client.

The following guest operating systems and Web browser versions are supported for the VMware Host Client.

Supported Browsers	Mac OS	Windows 32-bit and 64-bit	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	N/A
Safari	9.0+	N/A	N/A

Using the VMware Host Client

The embedded VMware Host Client is an HTML5-based client that is only used to manage single ESXi hosts. You can use the VMware Host Client to conduct an emergency management when vCenter Server is temporarily unavailable.

Start the VMware Host Client and Log In

You can use the VMware Host Client to manage single ESXi hosts and perform various administrative and troubleshooting tasks on your virtual machines.

Note: The VMware Host Client only works for administrative users.

1. In a Web browser enter the target host name or IP address using the form `http://host-name/ui` or `http://host-IP-address/ui`.

   A log in screen appears.
2. Enter your user name and your password.
3. Click **Login** to continue.
4. Review the VMware Customer Experience Improvement Program (CEIP) page and choose whether you want to join the program.

   To learn about the program and how to configure it at any time, see Configuring Customer Experience Improvement Program.
5. Click **OK**.

You are now logged in to your target ESXi host.

Log Out of the VMware Host Client

When you no longer need to view or manage your target ESXi host, log out of the VMware Host Client.

Note: Closing a VMware Host Client session does not stop the host.

To log out of the ESXi host, click the user name at the top of the VMware Host Client window and select **Log out** from the drop-down menu.

You are now logged out of the VMware Host Client. Your target ESXi host continues to run all its normal activities.

Configuring Customer Experience Improvement Program

You can participate in the Customer Experience Improvement Program (CEIP) to provide anonymous feedback or information to VMware for quality, reliability, and functionality improvments of VMware products and services.

VMware Customer Experience Improvement Program

VMware Tools participates in VMware's Customer Experience Improvement Program (CEIP).

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Leave and Rejoin the Customer Experience Improvement Program in the VMware Host Client

You can choose to leave the Customer Experience Improvement Program (CEIP), or rejoin the CEIP at any time.

1. To leave and rejoin the CEIP, click the user name at the top of the VMware Host Client page.
2. Point to **Client settings**> **Send usage statistics**, to leave or rejoin the CEIP.

Host Management with the VMware Host Client

With the VMware Host Client, you can manage single ESXi hosts during vCenter Server upgrades or when vCenter Server stops responding or becomes unavailable.

The VMware Host Client has a crucial set of troubleshooting functions, which allow you to perform tasks on the ESXi host that you are logged in to if vCenter Server is unavailable. These functions include but are not limited to configuring advanced host settings, licensing, managing certificates, using the ESXi Shell, enabling Lockdown mode, and so on.

Managing System Settings in the VMware Host Client

With the VMware Host Client, you can manage advanced host settings, assign or remove licenses to your host, configure start and stop policies for host services, and manage time and date configuration for the host.

Manage Advanced Settings in the VMware Host Client

You can change the settings of a host by using the VMware Host Client.

CAUTION: Changing advanced options is considered unsupported unless VMware technical support or a KB article instruct you to do so. In all other cases, changing these options is considered unsupported. In most cases, the default settings produce the optimum result.

1. Click **Manage** in the inventory and click **System**.
2. Click **Advanced settings**.
3. Right-click the appropriate item from the list and select **Edit option** from the drop-down menu.
   The **Edit option** dialog box is displayed.
4. Edit the value and click **Save** to apply your changes.
5. Optional: Right-click the appropriate item from the list and select **Reset to default** to go back to the original settings of the item.

Create an Initial Welcome Message for the Direct Console User Interface and the VMware Host Client

By using the VMware Host Client, you can create a welcome message that appears on the initial screen of the Direct Console User Interface (DCUI) and on the login window of the VMware Host Client. You can also create a welcome message that appears after a user logs into the VMware Host Client and decide whether to display the welcome message.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

Option	Action
Create a welcome message that appears before you log in to DCUI and VMware Host Client	1. Enter `Annotations.WelcomeMessage` in the **Search** text box and click the **Search** icon. 2. Right-click `Annotations.WelcomeMessage` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens.

Option	Action
	3. In the **New value** text box, enter the welcome message. To set the default message, leave the **New value** text box blank.
Create a welcome message that appears after you log in to the VMware Host Client	1. Enter `UserVars.HostClientWelcomeMessage` in the **Search** text box and click the **Search** icon. 2. Right-click `UserVars.HostClientWelcomeMessage` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. 3. In the **New value** text box, enter the welcome message. To set the default message, leave the **New value** text box blank.
Enable or disable the appearance of the welcome message after you log in to the VMware Host Client	1. Enter `UserVars.HostClientEnableMOTDNotification` in the **Search** text box and click the **Search** icon. 2. Right-click `UserVars.HostClientEnableMOTDNotification` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. 3. In the **New value** text box, enter the new value. A value of zero (0) disables the appearance of the welcome message. A value of one (1) enables the appearance of the welcome message.

2. Click **Save**.
3. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure the VMware Host Client User Interface Session Timeout

In VMware Host Client, the User Interface session automatically times out every 15 minutes and then you must log back in to the VMware Host Client.

You can increase the default inactivity timeout by changing an advanced configuration parameter. The default value is 900 seconds.

Configure the User Interface session timeout.

Option	Action
From the VMware Host Client Advanced Settings	1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings** 2. Enter `UserVars.HostClientSessionTimeout` in the **Search** text box and click the **Search** icon. 3. Right-click `UserVars.HostClientSessionTimeout` and select **Edit option** from the drop-down menu. The **Edit option** dialog box opens. 4. In the **New value** text box, enter the timeout setting in seconds. **Note:** A value of zero (0) disables the timeout. 5. Click **Save**. 6. To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.
From the User Settings drop-down menu	1. Click the user name at the top of the VMware Host Client window and select **Settings** > **Application timeout** > **.**

Option	Action
	2. To specify the inactivity timeout, select the time. 3. To disable the inactivity timeout, select Off.

Configure the SOAP Session Timeout in the VMware Host Client

In VMware Host Client you can configure the SOAP session timeout.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter `Config.HostAgent.vmacore.soap.sessionTimeout` in the **Search** text box and click the **Search** icon.
3. Right-click `Config.HostAgent.vmacore.soap.sessionTimeout` and select **Edit option** from the drop-down menu.

   The **Edit option** dialog box opens.
4. In the **New value** text box, enter the timeout setting in seconds.

   A value of zero (0) deactivates the timeout.
5. Click **Save**.
6. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure the Passwords and Account Lockout Policy in the VMware Host Client

For ESXi hosts, you must use a password with predefined requirements. You can change the required password length, character class requirements, or allow passphrases, all using the Security.PasswordQualityControl advanced option. You can also set the number of passwords to remember for each user using the Security.PasswordHistory advanced option. The Security.PasswordMaxDays advanced option allows you to set up the maximum number of days between password changes.

Note: Always perform additional testing after you change the default password settings.

If you attempt to log in with incorrect credentials, the account lockout policy specifies when and for how long the system locks your account.

ESXi Passwords

ESXi enforces password requirements for access.

- By default, when you create a password, you must include a mix of characters from any three of the following four character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash.
- By default, the password must contain a length of at least 7 characters and a maximum of 40 characters.
- Passwords must not contain a dictionary word or part of a dictionary word.
- Passwords must not contain the user name or parts of the user name.

Note:

An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

Example of ESXi Passwords

The following password candidates illustrate potential passwords if the option is set as follows:

```
retry=3 min=disabled,disabled,disabled,7,7
```

With this setting, a user is prompted up to three times (retry=3) for a new password that is not sufficiently strong or if the password was not entered correctly twice. Passwords with one or two character classes and password phrases are not allowed, because the first three items are deactivated. Passwords from three and four character classes require 7 characters.

The following password candidates meet the password requirements:

- xQaTEhb!: Contains eight characters from three character classes.
- xQaT3#A: Contains seven characters from four character classes.

The following password candidates do not meet the password requirements:

- Xqat3hi: Begins with an uppercase character, reducing the effective number of character classes to two. The minimum number of required character classes is three.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. The minimum number of required character classes is three.

Password Quality Control

You can control the quality of passwords by using the Security.PasswordQualityControl advanced option.

Security.PasswordQualityControl consists of several settings that follow the pattern:

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N simi-
lar=permit|deny
```

Password Quality Control Settings	Description	Default
`retry=N`	The number of times the user must provide a new password if the password is incorrect or not sufficiently strong.	`retry=3`
`min=N0,N1,N2, N3,N4`	Character class and the passphrase minimum length requirement. • `N0` is minimum length of passwords from a single character class. • `N1` is minimum length of passwords from two character classes.	`min=disabled,d isabled,disabl ed,7,7`

Password Quality Control Settings	Description	Default
	• N2 is minimum length for a passphrase. • N3 is minimum length for three character classes. • N4 is minimum length for four character classes. You can use disabled to disallow a password with the specified number of character classes.	
max=N	The maximum allowed password length.	max=40
passphrase=N	The number of words required for a passphrase. To make sure that the passphrase is recognized, do not set N2 from the min setting to disabled.	passphrase=3
similar=permit|deny	Indicates whether a password is allowed to be similar to the old password. To use this setting, make sure that you set the Security.PasswordHistory option to a non-zero value.	similar=deny

ESXi Passphrase

Instead of a password, you can use a passphrase. Passphrases are deactivated by default. You can change the default setting by using the Security.PasswordQualityControl advanced option.

For example, you can change the option to the following.

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows passphrases of at least 16 characters. The passphrase must consist of at least 3 words, separated by spaces.

Example Password History and Rotation Policy

To remember a history of 5 passwords, set the Security.PasswordHistory option to 5.

To enforce a 90 day password rotation policy, set the Security.PasswordMaxDays option to 90.

ESXi Account Lockout Policy	Users are locked out after a preset number of consecutive failed attempts. By default, users are locked out after 5 consecutive failed attempts in 3 minutes and a locked account is unlocked automatically after 15 minutes by default. You can change the maximum allowed failed attempts and the period of time in which the user account is locked out by using the Security.AccountLockFailures and Security.AccountUnlockTime advanced options.

To configure the administrator passwords and account lockout behaviour, perform the following steps.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.

Option	Action
Configure the required password length, character class requirement, or allow passphrases	1. Enter `Security.PasswordQualityControl` in the **Search** text box and click the **Search** icon. 2. Right-click `Security.PasswordQualityControl` and select **Edit option** from the drop-down menu.
Configure the number of passwords to remember for each user	1. Enter `Security.PasswordHistory` in the **Search** text box and click the **Search** icon. 2. Right-click `Security.PasswordHistory` and select **Edit option** from the drop-down menu. **Note:** Zero deactivates password history.
Configure the maximum number of days between password changes	1. Enter `Security.PasswordMaxDays` in the **Search** text box and click the **Search** icon. 2. Right-click `Security.PasswordMaxDays` and select **Edit option** from the drop-down menu.
Configure the number of failed login attempts allowed before lockout	1. Enter `Security.AccountLockFailures` in the **Search** text box and click the **Search** icon. 2. Right-click `Security.AccountLockFailures` and select **Edit option** from the drop-down menu. **Note:** Zero (0) deactivates account locking.
Configure the period of time in which the user's account is locked out	1. Enter `Security.AccountUnlockTime` in the **Search** text box and click the **Search** icon. 2. Right-click `Security.AccountUnlockTime` and select **Edit option** from the drop-down menu.

The **Edit option** dialog box opens.

2. In the **New value** text box, enter the new setting.
3. Click **Save**.
4. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure Syslog in theVMware Host Client

To configure the syslog service, you can use theVMware Host Client.

1. Click **Manage** in theVMware Host Client inventory and click **Advanced Settings**.
2. In the **Search** text box, enter the name of the setting that you want to change and click the **Search** icon.

Option	Description
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and the port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `protocol://hostName1:port` where `protocol` can be udp, tcp, or ssl. You can use only port 514 for UDP. The ssl protocol uses TLS 1.2. For example: `ssl://hostName1:1514` . The value of `port` can be any decimal number between 1 and 65535. While no hard limit to the number of remote hosts to receive syslog messages exists, it is recommended to keep the number of remote hosts to five or less.
Syslog.global.logCheckSSLCerts	Enforce checking of the SSL certificates when you log in to a remote host.
Syslog.global.defaultRotate	Maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. Specify the directory as [*`datastorename`*] *`path_to_file`*, where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of theESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.

3. Right-click the setting name and select **Edit option** from the drop-down menu.
   The **Edit option** dialog box opens.
4. To perform the SSL certificates check when you log in to a remote host, click **True** from the **New value**.
5. Click **Save**.
6. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure Advanced TLS/SSL Key Options

You can configure the security protocols and cryptographic algorithms that are used to encrypt communications with the ESXi host.

The Transport Layer Security (TLS) key secures communication with the host using the TLS protocol. Upon first boot, the ESXi host generates the TLS key as a 2048-bit RSA key. Currently, ESXi does not implement automatic generation of ECDSA keys for TLS. The TLS private key is not intended to be serviced by the administrator.

The SSH key secures communication with the ESXi host using the SSH protocol. Upon first boot, the system generates the SSH key as a 2048-bit RSA key. The SSH server is deactivated by default. SSH access is intended primarily for troubleshooting purposes. The SSH key is not intended to be serviced by the administrator. Logging in through SSH requires administrative privileges equivalent to full host control. To enable SSH access, see Enable the Secure Shell (SSH) in the VMware Host Client.

You can configure the following ESXi host security key settings.

Key	Default	Description
UserVars.ESXiVPsAllowedCiphers	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	The default cipher control string.
UserVars.ESXiVPsDisabledProtocols	sslv3,tlsv1,tlsv1.1	By default enables TLS v1.0, v1.1, and v1.2 protocols. SSL v3.0 is disabled. If you do not specify a protocol, all protocols are enabled.
Config.HostAgent.ssl.keyStore.allowAny	False	You can add any certificate to the ESXi CA trust store.
Config.HostAgent.ssl.keyStore.allowSelfSigned	False	You can add non-CA self-signed certificates to the ESXi CA trust store, that is, certificates that do not have the CA bit set.
Config.HostAgent.ssl.keyStore.discardLeaf	True	Discards leaf certificates added to the ESXi CA trust store.

To configure the ESXi security key settings:

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter the security key in the **Search** text box and click the **Search** icon.
3. Right-click the security key and select **Edit option** from the drop-down menu.
   The **Edit option** dialog box opens.
4. In the **New value** field entre the new value and click **Save**.
5. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Configure Userworld Memory Zeroing

With VMware Host Client, you can use the advanced option Mem.MemEagerZero to determine how pages are zeroed out for virtual machines and user space applications.

To zero all pages when they allocated to virtual machines and user space applications, set Mem.MemEagerZero to one (1). If the memory is not reused, this setting prevents exposing the information from a virtual machine or user space applications to other clients while preserving the previous content in memory.

When you set Mem.MemEagerZero to 1, pages are zeroed when a user space application exits. For virtual machines, such pages are zeroed if:

- The virtual machine is powered off.
- The virtual machine pages are migrated.
- The ESXi host reclaims virtual machines memory.

Note: For virtual machines, you can obtain this behaviour by setting the sched.mem.eagerZero advanced option to `TRUE`.

For information about setting the advanced virtual machine options, see the *vSphere Resource Management* documentation.

To configure the userworld memory zeroing, perform the following steps.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter `Mem.MemEagerZero` in the **Search** text box and click the **Search** icon.
3. Right-click `Mem.MemEagerZero` and select **Edit option** from the drop-down menu.
   The **Edit option** dialog box opens.
4. In the **New value** text box, enter the new value.

   The default value is zero (0).
5. Click **Save**.
6. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Change Autostart Configuration in theVMware Host Client

Configure autostart options for theESXi host to set up when the host starts and stops.

1. Click **Manage** in the inventory and click **System**.
2. Click **Autostart**.
3. Click **Edit settings**.
4. Select **Yes** to enable changing the autostart configuration.

Option	Description
Start delay	After you start theESXi host, it starts powering on the virtual machines that are configured for automatic startup. After theESXi host powers on the first virtual machine, the host waits for the specified delay time and then powers on the next virtual machine.
Stop delay	Stop delay is the maximum time theESXi host waits for a shutdown command to complete. The order in which virtual machines are shut down is the reverse of their startup order. After theESXi host shuts down the first virtual machine within the time that you specify, the host shuts down the next virtual machine. If a virtual machine does not shut down within the specified delay time, the host runs a power off command and then starts shutting down the next virtual machine. TheESXi host shuts down only after all virtual machines are shut down.
Stop action	Select a shut down action that is applicable to the virtual machines on the host when the host shuts down. • **System default** • **Power off** • **Suspend** • **Shut down**
Wait for heartbeat	Select **Yes** to enable the **Wait for heartbeat** option. You can use this option if the guest operating system of the virtual machine has VMware Tools installed. After theESXi host powers on the first virtual machine, the host immediately powers on the next virtual machine. The startup order in which

Option	Description
	virtual machines are powered on continues after the virtual machine receives the first heartbeat.

If you set a delay option to `-1` , the system uses the default option.

5. Click **Save**.

Edit the Time Configuration of anESXi Host in theVMware Host Client

By using theVMware Host Client, you can configure the time settings of a host manually or can synchronize the time and date of the host with an NTP or a PTP server. NTP provides millisecond timing accuracy and PTP maintains microsecond timing accuracy.

The NTP service on the host periodically takes the time and date from the NTP server. You can use the **Start**, **Stop**, or **Restart** buttons to change the status of the NTP service on the host at any time regardless of the selected startup policy for the NTP service.

PTP provisions precise time synchronization for the virtual machines within a network. To change the PTP service on the host at any time, you can use the **Start**, **Stop**, or **Restart** buttons. Starting or stopping the PTP service automatically enables or disables PTP. To apply the change when you enable or disable PTP manually, start or stop the PTP service.

For more information about services, see Manage Services in the VMware Host Client.

Note: The NTP and PTP services cannot run simultaneously.

1. Click **Manage** in theVMware Host Client inventory.
2. On the **System** tab, click **Time & date**.
3. Set the time and date for the host.

Option	Action
Manually configure the date and time on this host	1. Click **Edit NTP Settings**. The **Edit NTP Settings** dialog box appears. 2. Set the time and date for the host manually. 3. Click **Save**.
Use Network Time Protocol (Enable NTP client)	1. Click **Edit NTP Settings**. The **Edit NTP Settings** dialog box appears. 2. Select the **Use Network Time Protocol** radio button. 3. In the **NTP Servers** text box, enter the IP addresses or host names of the NTP servers that you want to use. 4. From the **NTP Service Startup Policy** drop-down menu, select an option for starting and stopping the NTP service on the host. – **Start and stop with port usage**. Starts or stops the NTP service when the NTP client port is enabled or disabled for access in the security profile of the host. – **Start and stop with host**. Starts and stops the NTP service when the host powers on and shuts down. – **Start and stop manually**. Enables manual starting and stopping of the NTP service. If you select the **Start and stop manually** policy, the status of the NTP service changes only when you use the UI controls. 5. Click **Save**.
Use Precision Time Protocol (Enable PTP client)	1. Click **Edit PTP Settings**. 2. Select the **Enable** check box.

Option	Action
	3. From the **Network interface** drop-down menu, select a network interface. The IPv4 and Subnet mask appear. 4. Click **Save**.

Managing Hardware for an ESXi Host by Using the VMware Host Client

When you log in to an ESXi host by using the VMware Host Client, you can manage PCI devices and configure power management settings.

Host Power Management Policies

You can apply several power management features in ESXi that the host hardware provides to adjust the balance between performance and power. You can control how ESXi uses these features by selecting a power management policy.

Selecting a high-performance policy provides more absolute performance, but at lower efficiency and performance per watt. Low-power policies provide less absolute performance, but at higher efficiency.

You can select a policy for the host that you manage by using the VMware Host Client. If you do not select a policy, ESXi uses Balanced by default.

Table 524: CPU Power Management Policies

Power Management Policy	Description
High Performance	Do not use any power management features.
Balanced (Default)	Reduce energy consumption with minimal performance compromise
Low Power	Reduce energy consumption at the risk of lower performance
Custom	User-defined power management policy. Advanced configuration becomes available.

When a CPU runs at lower frequency, it can also run at lower voltage, which saves power. This type of power management is typically called Dynamic Voltage and Frequency Scaling (DVFS). ESXi attempts to adjust CPU frequencies so that virtual machine performance is not affected.

When a CPU is idle, ESXi can apply deep halt states, also known as C-states. The deeper the C-state, the less power the CPU uses, but it also takes longer for the CPU to start running again. When a CPU becomes idle, ESXi applies an algorithm to predict the idle state duration and chooses an appropriate C-state to enter. In power management policies that do not use deep C-states, ESXi uses only the shallowest halt state for idle CPUs, C1.

Change Power Management Policies in the VMware Host Client

Change the power management policies of the host that you are managing to control the energy consumption of your host.

1. Click **Manage** in the VMware Host Client inventory and click **Hardware.**
2. Click **Power Management** and click **Change policy**.
   The available power management policies are displayed.

3. Select the radio button next to the policy that you want to apply.
4. Click **OK**.

Change the Hardware Label in the VMware Host Client

In the VMware Host Client, you can change the hardware label of all available PCI passthrough devices on a virtual machine. You use hardware labels to restrict the virtual machine placement to specific hardware instances. You can add all available devices with the same hardware label or with a blank hardware label to a virtual machine.

1. Click **Manage** in the VMware Host Client inventory.
2. On the **Hardware** tab, click **PCI Devices**.
3. Select an available device from the list and click **Hardware label**.
   The toggle passthrough must be active for the selected device.
   The **Edit Hardware Label** dialog box appears.
4. Edit the hardware label and click **Save** to apply the changes.

The new hardware label appears in the hardware label column.

Licensing for ESXi Hosts

ESXi hosts are licensed with vSphere licenses. Each vSphere license has a certain capacity that you can use to license multiple physical CPUs on ESXi hosts.

Starting with vSphere 7.0, one CPU license covers one CPU with up to 32 cores. If a CPU has more than 32 cores, you need additional CPU licenses.

Number of CPUs	Cores per CPU	Number of CPU Licenses
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

When you assign a vSphere license to a host, the amount of capacity consumed is determined by the number of physical CPUs on the host and the number of physical cores in each physical CPU.

vSphere Desktop that is intended for VDI environments is licensed on per virtual machine basis.

To license an ESXi host, you must assign it a vSphere license that meets the following prerequisites:

- The license must have sufficient capacity to license all physical CPUs on the host.
- The license must support all the features that the host uses. For example, if the host is associated with a vSphere Distributed Switch, the license that you assign must support the vSphere Distributed Switch feature.

If you attempt to assign a license that has insufficient capacity or does not support the features that the host uses, the license assignment fails.

If you use the licensing model with up to 32 cores, you can assign a vSphere license for 10 32-core CPUs to any of the following combinations of hosts:

- Five 2-CPU hosts with 32 cores per CPU
- Five 1-CPU hosts with 64 cores per CPU
- Two 2-CPU hosts with 48 cores per CPU and two 1-CPU hosts with 20 cores per CPU

Dual-core and quad-core CPUs, such as Intel CPUs that combine two or four independent CPUs on a single chip, count as one CPU.

Evaluation Mode

After you install ESXi, it operates in evaluation mode for up to 60 consecutive days. An evaluation mode license provides all features of the highest vSphere product edition.

After you assign a license to an ESXi host, at any time before the evaluation period expires, you can set the host back to evaluation mode to explore the entire set of features available for the remaining evaluation period.

For example, if you use an ESXi host in evaluation mode for 20 days, then assign a vSphere Standard license to the host, and 5 days later set the host back to evaluation mode, you can explore the entire set of features available for the host for the remaining 35 days of the evaluation period.

License and Evaluation Period Expiry

For ESXi hosts, license or evaluation period expiry leads to disconnection from vCenter Server. All powered on virtual machines continue to work, but you cannot power on virtual machines after they are powered off. You cannot change the current configuration of the features that are in use. You cannot use the features that remained unused before the license expiration.

Note: When there are expiring licenses, a notification appears 90 days before the license expiration.

Licensing ESXi Hosts After Upgrade

If you upgrade an ESXi host to a version that starts with the same number, you do not need to replace the existing license with a new one. For example, if you upgrade a host from ESXi 5.1 to 5.5, you can use the same license for the host.

If you upgrade an ESXi host to a major version that starts with a different number, the evaluation period restarts and you must assign a new license. For example, if you upgrade an ESXi host from 5.x to 6.x, you must license the host with a vSphere 6 license.

vSphere Desktop

vSphere Desktop is intended for VDI environments such as Horizon View. The license use for vSphere Desktop equals the total number of powered on desktop virtual machines running on the hosts that are assigned a vSphere Desktop license.

View Licensing Information About the VMware Host Client Environment

You can view the available licenses in the VMware Host Client along with their expiration dates, license key, and various features. You can also view the available products and assets.

Click **Manage** in the VMware Host Client inventory and click **Licensing**.

You can view the license key, the expiration date, and all the available features and assets.

Assign a License Key to an ESXi Host in the VMware Host Client

By using the VMware Host Client, you can assign an existing or new license key to an ESXi host.

Verify that you have the **Global** > **Licenses** privilege.

Note: If you use vCenter Server to manage your ESXi host, you can only change your licenses from the vSphere Client.

1. Click **Manage** in the VMware Host Client inventory and click **Licensing**.
2. Click **Assign license**, enter a license key in the form *XXXXX-XXXXX-XXXXX-XXXXX-XXXXX*, and click **Check license**.
3. Click **Assign license** to save your changes.

Remove a License from an ESXi Host in the VMware Host Client

To remain in compliance with the licensing models of products that you use with vSphere, you must remove all unassigned licenses from the inventory. If you have divided, combined, or upgraded licenses in Customer Connect, you must remove the old licenses.

For example, suppose that you have upgraded a vSphere license from 6.5 to 6.7 in Customer Connect. You assign the license to ESXi 6.7 hosts. After assigning the new vSphere 6.7 licenses, you must remove the old vSphere 6.5 license from the inventory.

1. Click **Manage** in the VMware Host Client inventory and click **Licensing**.
2. Click **Remove license**, and click **OK**.

Manage Services in the VMware Host Client

In the VMware Host Client, you can start, stop, and restart services that are running on the host that you are logged in to, and you can configure host service policy. You can restart services when you change host configurations or in case of suspected functional or performance issues.

1. Click **Manage** in the VMware Host Client inventory and click **Services**.
2. From the **Services** list, select a service.
3. From the **Actions** drop-down menu, select an operation.
   - **Restart**
   - **Start**
   - **Stop**
4. Optional: From the **Actions** drop-down menu, select **Policy** and select an option for the service from the menu.
   - **Start and stop with firewall ports**
   - **Start and stop with host**
   - **Start and stop manually**

Managing Security and Users for an ESXi Host by Using the VMware Host Client

The ESXi hypervisor architecture has many built-in security features that you can configure to enhance security. By using the VMware Host Client, you can configure features, such as active directory, and you can also manage certificates.

Managing Host Authentication by Using the VMware Host Client

When you log in to an ESXi host by using the VMware Host Client, you can check whether active directory and smart card authentication are enabled, and you can also join the host to a directory service domain.

Join an ESXi Host to a Directory Service Domain by Using the VMware Host Client

To use a directory service for your host, you must join the host to the directory service domain.

You can enter the domain name in one of two ways:

- `name.tld` (for example, `domain.com`): The account is created under the default container.
- `name.tld/container/path` (for example, `domain.com/OU1/OU2`): The account is created under a particular organizational unit (OU).

To use the vSphere Authentication Proxy service, see *vSphere Security*.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Authentication** and click **Join domain**.
3. Enter a domain name.

   Use the form `name.tld` or `name.tld/container/path`.
4. Enter the user name and password of a directory service user account that has permissions to join the host to the domain and click **Join domain**.
5. Optional: If you intend to use an authentication proxy, enter the proxy server IP address and click **Join domain**.

Using Active Directory to Manage ESXi Users

You can configure ESXi to use a directory service such as Active Directory to manage users.

Creating local user accounts on each host presents challenges with having to synchronize account names and passwords across multiple hosts. Join ESXi hosts to an Active Directory domain to eliminate the need to create and maintain local user accounts. Using Active Directory for user authentication simplifies the ESXi host configuration and reduces the risk for configuration issues that could lead to unauthorized access.

When you use Active Directory, users supply their Active Directory credentials and the domain name of the Active Directory server when adding a host to a domain.

Using vSphere Authentication Proxy

You can add ESXi hosts to an Active Directory domain by using vSphere Authentication Proxy instead of adding the hosts explicitly to the Active Directory domain.

You only have to set up the host so it knows about the domain name of the Active Directory server and about the IP address of vSphere Authentication Proxy. When vSphere Authentication Proxy is enabled, it automatically adds hosts that are being provisioned with Auto Deploy to the Active Directory domain. You can also use vSphere Authentication Proxy with hosts that are not provisioned by using Auto Deploy.

Auto Deploy	If you are provisioning hosts with Auto Deploy, you can set up a reference host that points to Authentication Proxy. You then set up a rule that applies the reference host's profile to any ESXi host that is provisioned with Auto Deploy. vSphere Authentication Proxy stores the IP addresses of all hosts that Auto Deploy provisions using PXE in its access control list. When the host boots, it contacts vSphere Authentication Proxy, and vSphere Authentication Proxy joins those hosts, which are already in its access control list, to the Active Directory domain. Even if you use vSphere Authentication Proxy in an environment that uses certificates that are provisioned by VMCA or third-party certificates, the process works seamlessly if you follow the instructions for using custom certificates with Auto Deploy.
Other ESXi Hosts	You can set up other hosts to use vSphere Authentication Proxy if you want to make it possible for the host to join the domain without using Active Directory credentials. That means you do not need to transmit Active Directory credentials to the host, and you do not save Active Directory credentials in the host profile.

In that case, you add the host's IP address to the vSphere Authentication Proxy access control list, and vSphere Authentication Proxy authorizes the host based on its IP address by default. You can enable client authentication to have vSphere Authentication Proxy check the host's certificate.

Note: You cannot use vSphere Authentication Proxy in an environment that supports only IPv6.

Managing Host Certificates by Using the VMware Host Client

When you log in to an ESXi host by using the VMware Host Client, you can view the certificate details of your host, such as the issuer and the validity period, and you can also import new certificates

View Certificate Details for anESXi Host in theVMware Host Client

You can use the certificate information for debugging.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Certificates**.
   You can view the following certificate details.

Field	Description
Issuer	The issuer of the certificate.
Not valid after	Date on which the certificate expires.
Not valid before	Date on which the certificate is generated.
Subject	The subject used during certificate generation.

Import a New Certificate for an ESXi Host in the VMware Host Client

You can import a certificate from a trusted certificate authority when you are logged in to an ESXi host with the VMware Host Client.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Certificates** and click **Import new certificate**.
3. Generate a certificate signing request:

Option	Description
Generate FQDN signing request	• Click **Generate FQDN signing request**, click the **Copy to clipboard** button, and click **Close**. • To generate the signed certificate, pass the certificate signing request to the certificate authority (CA). • In the **Certificate** text box, paste the generated signed certificate in PEM format and click **Import**.
Generate IP signing request	• Click **Generate IP signing request**, click the **Copy to clipboard** button, and click **Close**.

Option	Description
	• To generate the signed certificate, pass the certificate signing request to the CA. • In the **Certificate** text box, paste the generated signed certificate in PEM format and click **Import**.

You do not have to import the certificate immediately. To make sure that you can use the signed certificate, do not restart the host between generating the certificate signing request and importing the certificate.

The certificate signing request is then passed to the certificate authority to generate the official certificate.

An FQDN request has the fully qualified host name of the host in the resulting common name field of the certificate. The IP signing request has the current IP address of the host in the common name field.

Managing Users with the VMware Host Client

Manage users to control who is authorized to log in to ESXi.

Users and roles control who has access to the ESXi host components and what actions each user can perform.

In vSphere 5.1 and later, ESXi user management has the following caveats .

- The users created when you connect directly to an ESXi host are not the same as the vCenter Server users. When the host is managed by vCenter Server, vCenter Server ignores users created directly on the host.
- You cannot create ESXi users by using the vSphere Client. You must log in to the host directly with the VMware Host Client to create ESXi users .
- ESXi 5.1 and later does not support local groups. However, Active Directory groups are supported.

To prevent anonymous users, such as root, from accessing the host with the Direct Console User Interface (DCUI) or ESXi Shell, remove the user's administrator privileges on the root folder of the host. This applies to both local users and Active Directory users and groups.

Add an ESXi User in the VMware Host Client

Adding a user to the users table updates the internal user list that the host maintains.

For information about password requirements, see Configure the Passwords and Account Lockout Policy in the VMware Host Client or the *vSphere Security* documentation.

1. Log in to ESXi with the VMware Host Client.

   You cannot create ESXi users with the vSphere Client. To create ESXi users, you must directly log in to the host with the VMware Host Client.

2. Click **Manage** in the inventory and click **Security & Users**.
3. Click **Users**.
4. Click **Add user**.
5. Enter a user name, and a password.

   Note: Do not create a user named `ALL`. Privileges associated with the name `ALL` might not be available to all users in some situations. For example, if a user named `ALL` has Administrator privileges, a user with the **ReadOnly** privileges might be able to log in to the host remotely. This is not the intended behavior.

   - Do not include any spaces in the user name.
   - Do not include any non-ASCII characters in the user name.
   - Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so` . If the password is not compliant, an error message indicates password requirements.
6. Click **Add**.

Update an ESXi User in the VMware Host Client

You can change the description and password for an ESXi user in the VMware Host Client.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Users**.
3. Select a user from the list and click **Edit user**.
4. Update the user details and click **Save**.

Remove a Local ESXi User from a Host in the VMware Host Client

You can remove a local ESXi user from the host.

CAUTION: Do not remove the root user.

If you remove a user from the host, they lose permissions to all objects on the host and cannot log in again.

Note: Users who are logged in and are removed from the domain keep their host permissions until you restart the host.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Users**.
3. Select the user that you want to remove from the list, click **Remove user**, and click **Yes**.

   Do not remove the root user for any reason.

Managing ESXi Roles in the VMware Host Client

ESXi grants access to objects only to users who are assigned permissions for the object. When you assign a user permission for the object, you do so by pairing the user with a role. A role is a predefined set of privileges. For more information about privileges, see the *vSphere Security* documentation.

ESXi hosts provide three default roles, and you cannot change the privileges associated with these roles. Each subsequent default role includes the privileges of the previous role. For example, the Administrator role inherits the privileges of the Read Only role. Roles that you create do not inherit privileges from any of the default roles.

You can create custom roles by using the role-editing functions in the VMware Host Client to create privilege sets that match your user needs. Also, the roles you create directly on a host are not accessible in vCenter Server. You can work with these roles only if you log in to the host directly from the VMware Host Client.

Note: When you add a custom role and do not assign any privileges to it, the role is created as a read-only role with the **System.Anonymous**, **System.View**, and **System.Read** system-defined privilege.

If you manage an ESXi host through vCenter Server, maintaining custom roles in the host and vCenter Server can result in confusion and misuse. In this type of configuration, maintain custom roles only in vCenter Server.

You can create host roles and set permissions through a direct connection to the ESXi host with the VMware Host Client.

Add a Role in the VMware Host Client

You can create roles to suit the access control needs of your environment.

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Roles**.
3. Click **Add role**.
4. Enter a name for the new role.
5. Select privileges from the list to associate with the new role and click **Add**.

Update a Role in the VMware Host Client

When you edit a role, you can change the privileges selected for that role. When complete, these privileges are applied to any user or group that is assigned the edited role.

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Roles**.
3. Select a role from the list and click **Edit role**.
4. Update the role details and click **Save**.

Remove a Role in the VMware Host Client

When you remove a role that is not assigned to any users or groups, the definition is removed from the list of roles. When you remove a role that is assigned to a user or group, you can remove assignments or replace them with an assignment to another role.

Verify that you are logged in as a user with Administrator privileges, such as root or vpxuser.

CAUTION: You must understand how users will be affected before removing all assignments or replacing them. Users who have no permissions granted to them cannot log in.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Roles**.
3. Select the name of the role that you want to remove from the list.
4. Click **Remove role**, select **Remove only if unused**, and click **Yes**.

Managing Hosts in vCenter Server

To monitor all hosts in your virtual environment from one place and to simplify host configuration, connect the hosts to a vCenter Server system.

For information about configuration management of ESXi hosts, see the *vSphere Networking* documentation, the *vSphere Storage* documentation, and the *vSphere Security* documentation.

Update Your VMware Host Client Environment to the Latest Version

To evaluate whether you are using the latest version of the VMware Host Client, check what VIBs are installed to your environment and examine the VIBs version information. You can update your VMware Host Client environment by entering a URL or a datastore path to either a VIB or the `metadata.zip` file in an ESXi offline bundle package.

If you provide a VIB file, an existing VIB that is installed to your VMware Host Client environment is updated to the new VIB.

If you provide an offline bundle, you update the entire ESXi host to the version described by the `metadata.zip` file in the bundle. Make sure that the entire offline bundle is available through the URL or is uploaded to the datastore.

To update your environment to the latest version, perform the following tasks:

Task	Steps
Upload a VIB to a datastore	1. Click **Storage** from the VMware Host Client environment. 2. Select a datastore from the list and click **Datastore browser**. 3. To store the VIB, select a directory and click **Upload**. 4. Browse to and double-click the file.
Upload an offline bundle to a datastore	1. Download the ESXi offline bundle package. 2. Upload the ESXi offline bundle package to the ESXi host. You can either upload the offline bundle package by using the **Datastore browser** or by using SCP or WinSCP. 3. Extract the contents of the offline bundle on the ESXi host. For example, log in to the host by using SSH. 4. Navigate to the directory where you uploaded the offline bundle. 5. Extract the contents by using the `unzip` command.
Update your environment	1. Click **Manage** in the VMware Host Client and click **Packages**. 2. Click **Install update** and enter the URL or the datastore path to a VIB or a `metadata.zip` file in an offline bundle. 3. Click **Update**. **CAUTION:** If you update an ESXi host managed by vSphere Lifecycle Manager, the host might become non-compliant. 4. Click **Refresh** to make sure that the update is successful.

Unable to Connect from the VMware Host Client to an ESXi Host After Upgrading to a Newer Version of ESXi

After you upgrade your host from ESXi to a newer version, your browser console might display an error message when you attempt to access your ESXi host by using the VMware Host Client, and your connection might fail.

After you upgrade your ESXi host to a newer version, attempting to navigate to `https://host-fqdn/ui` or `https://1.2.3.4/ui` might result in the following error:

```
503 Service Unavailable (Failed to connect to endpoint:
 [N7Vmacore4Http16LocalServiceSpecE:0xffa014e8] _serverNamespace = /ui _isRedirect = false
 _port = 8308)
```

A change to `/etc/vmware/rhttpproxy/endpoints.conf` remains after an upgrade and causes the `/ui` endpoint to override the VMware Host Client.

When the `/ticket` is missing from the `endpoint.conf` file on your 6.0 or later ESXi host, your in-browser virtual machine console displays a `Failed to connect` error message but the continues to work.

1. Log in to your ESXi host either by using SSH or ESXi Shell.

   If you use SSH, you might need to enable SSH first. You can enable SSH by using DCUI.

2. Back up the `endpoints.conf` file.

   ```
   cp /etc/vmware/rhttpproxy/endpoints.conf /tmp
   ```

3. Open the `/etc/vmware/rhttpproxy/endpoints.conf` file in an editor and remove the following line.

   ```
   /ui local 8308 redirect  allow
   ```

4. Restart the reverse Web proxy.

   ```
   /etc/init.d/rhttpproxy restart
   ```

5. Access the VMware Host Client using the host's specified full name in the secure URL with `https://host-fqdn/ui` or a valid numeric IP address `https://1.2.3.4/ui`.

Switch to the vSphere Client

To access the full set of capabilities, and advanced administrative and troubleshooting functions of the ESXi host, connect the ESXi host to vCenter Server.

1. Right-click **Host** in the VMware Host Client inventory and select **Manage with vCenter Server** from the drop-down menu.

   The vCenter Server login page opens in a new window.

2. Enter your credentials and click **Login**.

Disconnect an ESXi Host from vCenter Server by Using the VMware Host Client

If you no longer want to use the advanced set of capabilities available through vCenter Server for host management, or if vCenter Server has failed and you must perform emergency operations on the host, you can disconnect your ESXi host from vCenter Server.

Disconnecting an ESXi host might take up to several minutes.

1. Right-click **Host** in the VMware Host Client inventory and select **Disconnect from vCenter Server** from the pop-up menu.

   Note: Disconnecting a host signals vCenter Server that this host is not responding.

2. Click **Disconnect from vCenter Server**.

Reboot or Shut Down an ESXi Host in the VMware Host Client

You can power off or restart any ESXi host by using the VMware Host Client. Powering off a managed host disconnects it from vCenter Server, but does not remove it from the inventory.

To be able to reboot or shut down a host, you need these privileges.

- **Host** > **Configuration** > **Maintenance**
- **Global** > **Log event**

Always perform the following tasks before you reboot or shut down a host:

- Power off all virtual machines on the host.

- Place the host in maintenance mode.

1. Right-click the host, select **Shut down host** or **Reboot host**.

   Note: If the host is not in maintenance mode, shutting down or rebooting it does not stop the virtual machines that are running on this host safely and unsaved data may be lost. If the host is part of a cluster, you might lose access to the data on the host.

2. Click **Shut down** or **Reboot** to complete the procedure.

Using the ESXi Shell

The ESXi Shell is disabled by default on ESXi hosts. You can enable local and remote access to the shell if necessary.

To reduce the risk of unauthorized access, enable the ESXi Shell for troubleshooting only.

The ESXi Shell is independent of lockdown mode. Even if the host is running in lockdown mode, you can still log in to the ESXi Shell if it is enabled.

ESXi Shell	Enable this service to access the ESXi Shell locally.
SSH	Enable this service to access the ESXi Shell remotely by using SSH.

The root user and users with the Administrator role can access the ESXi Shell. Users who are in the Active Directory group ESX Admins are automatically assigned the Administrator role. By default, only the root user can run system commands (such as `vmware -v`) by using the ESXi Shell.

Note: Do not enable the ESXi Shell unless you actually need access.

Enable the Secure Shell (SSH) in the VMware Host Client

Enable the Secure Shell (SSH) to access the ESXi Shell remotely by using SSH.

1. To enable or disable the Secure Shell (SSH), right-click **Host** in the VMware Host Client inventory.
2. Select **Services** from the drop-down menu and select **Secure Shell (SSH)**.
3. Select a task to perform.
   - If SSH is enabled, click **Disable** to disable it.
   - If SSH is disabled, click **Enable** to enable it.

Enable the ESXi Console Shell in the VMware Host Client

When you enable this service while running in lockdown mode, you can log in locally to the direct console user interface as the root user and disable lockdown mode. You can then access the host using a direct connection to the VMware Host Client or by enabling the ESXi Shell.

1. To enable or disable the Console Shell, right-click **Host** in the VMware Host Client inventory.
2. Select **Services** from the drop-down menu and select **Console Shell**.
3. Select a task to perform.
   - If the Console Shell is enabled, click **Disable** to disable it.
   - If the Console Shell is disabled, click **Enable** to enable it.

Create a Timeout for ESXi Shell Availability in the VMware Host Client

The ESXi Shell is disabled by default. To increase security when you enable the shell, you can set an availability timeout for the ESXi Shell.

The availability timeout defines how long both local and remote shell logins are allowed before the ability to log in through the shell is disabled. When the availability timeout expires, any existing shell sessions remains, but new shell sessions are not allowed.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter `UserVars.ESXiShellTimeOut` in the **Search** text box and click the **Search** icon.
3. Right-click `UserVars.ESXiShellTimeOut` and select **Edit option** from the drop-down menu.
   The **Edit option** dialog box opens.
4. In the **New value** text box, enter the timeout setting.
   A value of zero (0) disables the timeout.
5. Click **Save**.
   You must restart the SSH service and the ESXi Shell service for the timeout to take effect.
6. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

Create a Timeout for Idle ESXi Shell Sessions in the VMware Host Client

If you enable the ESXi Shell on a host, but forget to log out of the session, the idle session remains connected indefinitely. The open connection increases the potential for someone to gain privileged access to the ESXi host. Prevent this by setting a timeout for idle sessions.

The idle timeout is the amount of time that can elapse before you are logged out of an idle interactive session.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Enter `UserVars.ESXiShellInteractiveTimeOut` in the **Search** text box and click the **Search** icon.
3. Right-click `UserVars.ESXiShellInteractiveTimeOut` and select **Edit option** from the drop-down menu.
   The **Edit option** dialog box opens.
4. In the **New value** text box, enter the timeout setting.
   A value of zero (0) disables the timeout.
5. Click **Save**.
   The timeout takes effect only for newly logged in sessions.
6. Optional: To reset the key setting to default, right-click the appropriate key from the list and select **Reset to default**.

If the session is idle, users are logged out after the timeout period elapses.

Place a Host in Maintenance Mode in the VMware Host Client

You place a host in maintenance mode when you need to service it, for example, to install more memory. A host enters or leaves maintenance mode only as the result of a user request.

Before you place a host in maintenance mode, power off all virtual machines that are running on that host or migrate them to another host either manually or automatically by DRS.

The host is in a state of **Entering Maintenance Mode** until all running virtual machines are powered off or migrated to different hosts. You cannot power off virtual machines or migrate virtual machines to a host that is entering or in maintenance mode.

To place a host in maintenance mode, all virtual machines that are running on the host must be powered off or migrated to different hosts. If you attempt to place a host that has running virtual machines on it in maintenance mode, DRS must power off or migrate the running virtual machines for the task to complete. If a time out occurs before the virtual machines are powered off or migrated, an error message appears.

When all virtual machines on the host are inactive, the host's icon displays **under maintenance** and the host's Summary panel indicates the new state. While in maintenance mode, the host does not allow you to deploy or power on a virtual machine.

Right-click the host and select **Enter maintenance mode**.

The host is in maintenance mode until you select **Exit maintenance mode**.

Managing Permissions in the VMware Host Client

For ESXi, permissions are defined as access roles that consist of the roles assigned to a user for different objects such as a virtual machine or ESXi host. Permissions grant users the right to perform the activities specified by the role on the object to which the role is assigned.

For example, to configure memory for the host, a user must be granted a role that includes the **Host** > **Configuration** > **Memory Configuration** privilege. By assigning different roles to users for different objects, you can control the tasks that users can perform by using the VMware Host Client.

When connecting directly to a host with the VMware Host Client, the root and vpxuser user accounts have the same access rights as any user assigned the Administrator role on all objects.

All other users initially have no permissions on any object, which means the users cannot view or perform tasks on these objects. A user with Administrator privileges must assign permissions to these users to allow them to perform tasks.

Many tasks require permissions on more than one object. The following rules can help you determine which roles to assign to users to allow particular tasks:

- Any task that consumes hard disk space, such as creating a virtual disk or taking a snapshot, requires the **Datastore** > **Allocate Space** privilege on the target datastore and the privilege to perform the operation itself.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource** > **Assign Virtual Machine to Resource Pool** privilege.

The list of privileges is the same for both ESXi and vCenter Server.

You can create roles and set permissions through a direct connection to the ESXi host.

Permission Validation

vCenter Server and ESXi hosts that use Active Directory regularly validate users and groups against the Windows Active Directory domain. Validation occurs whenever the host system starts and at regular intervals specified in the vCenter Server settings.

For example, if user Smith was assigned permissions and in the domain the user’s name was changed to Smith2, the host concludes that Smith no longer exists and removes permissions for that user when the next validation occurs.

Similarly, if user Smith is removed from the domain, all permissions are removed when the next validation occurs. If a new user Smith is added to the domain before the next validation occurs, the new user Smith receives all the permissions the old user Smith was assigned.

Assign Permissions to a User for an ESXi Host in the VMware Host Client

To perform particular activities on an ESXi host, a user must have permissions that are associated with a particular role. In the VMware Host Client, you can assign roles to users and give the users the permissions necessary to perform various tasks on the host.

1. Right-click **Host** in the VMware Host Client inventory and click **Permissions**.
2. Click **Add user**.
3. Click the arrow next to the **Select a user** text box and select the user that you want to assign a role to.
4. Click the arrow next to the **Select a role** text box and select a role from the list.
5. Optional: Select **Propagate to all children** or **Add as group**.

   If you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and other objects in the vCenter Server instance.
6. Click **Add** and click **Close**.

Remove Permissions for a User in the VMware Host Client

Removing a permission for a user does not remove the user from the list of users available. It also does not remove the role from the list of available items. It removes the user and role pair from the selected inventory object.

1. Right-click **Host** in the VMware Host Client inventory and click **Permissions**.
2. Select a user from the list and click **Remove user**.
3. Click **Close**.

Assign a User Permissions for a Virtual Machine in the VMware Host Client

Assign a role to a particular user to give that user permissions to perform specific tasks on a virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine from the list and select **Permissions**.
3. Click **Add user**.
4. Click the arrow next to the **Select a user** text box and select the user that you want to assign a role for.
5. Click the arrow next to the **Select a role** text box and select a role from the list.
6. Optional: Select **Propagate to all children**.

   If you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and similar objects in the vCenter Server instance.

7. Click **Add** and click **Close**.

Remove Permissions for a Virtual Machine in the VMware Host Client

To make a user unable to perform tasks on a particular virtual machine, remove the permissions of the user for that virtual machine.

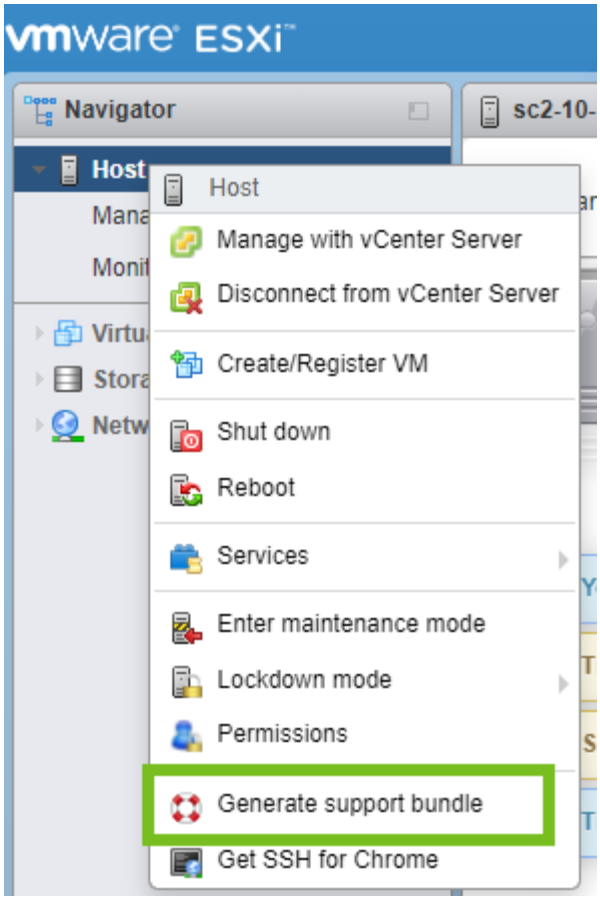
Removing a permission for a user does not remove the user from the list of users available. It also does not remove the role from the list of available items. It removes the user and role pair from the selected inventory object.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine from the list and select **Permissions**.
3. Select a user from the list and click **Remove user**.
4. Click **Close**.

Generate a Support Bundle in the VMware Host Client

You can generate a support bundle for the ESXi host that you are logged in on. The support bundle contains the log files and system information that you can use to diagnose and resolve problems.

1. Right-click **Host** in the VMware Host Client inventory and select **Generate support bundle** from the drop-down menu.



   A dialog box that contains a link to download the bundle pops up when the support bundle is created.

2. Optional: Click **Monitor** in the VMware Host Client inventory, click **Tasks**, and click a log bundle from the list.
   You can view the link to the log bundle under the table.

Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode. In lockdown mode, operations must be performed through vCenter Server by default.

Normal Lockdown Mode and Strict Lockdown Mode

With vSphere 6.0 and later, you can select normal lockdown mode or strict lockdown mode.

Normal Lockdown Mode	In normal lockdown mode, the DCUI service remains active. If the connection to the vCenter Server system is lost, and access through the vSphere Client is unavailable, privileged accounts can log in to the ESXi host's Direct Console Interface and exit lockdown mode. Only the following accounts can access the Direct Console User Interface: • Accounts in the Exception User list for lockdown mode who have administrative privileges on the host. The Exception Users list is meant for service accounts that perform specific tasks. Adding ESXi administrators to this list defeats the purpose of lockdown mode. • Users defined in the DCUI.Access advanced option for the host. This option is for emergency access to the Direct Console Interface in case the connection to vCenter Server is lost. These users do not require administrative privileges on the host.
Strict Lockdown Mode	In strict lockdown mode, the DCUI service is stopped. If the connection to vCenter Server is lost and the vSphere Client is no longer available, the ESXi host becomes unavailable, unless the ESXi Shell and SSH services are enabled and Exception Users are defined. If you cannot restore the connection to the vCenter Server system, you must reinstall the host.

Lockdown Mode and the ESXi Shell and SSH Services

Strict lockdown mode stops the DCUI service. However, the ESXi Shell and SSH services are independent of lockdown mode. For lockdown mode to be an effective security measure, ensure that ESXi Shell and SSH services are also disabled. These services are disabled by default.

When a host is in lockdown mode, users on the Exception Users list can access the host from the ESXi Shell and through SSH if they have the Administrator role on the host. This access is possible even in strict lockdown mode. Leaving the ESXi Shell service and the SSH service disabled is the most secure option.

Note: The Exception Users list is meant for service accounts that perform specific tasks such as host backups, and not for administrators. Adding administrator users to the Exception Users list defeats the purpose of lockdown mode.

Put an ESXi Host in Normal Lockdown Mode by Using the VMware Host Client

You can use the VMware Host Client to enter normal lockdown mode.

1. Right-click **Host** in the VMware Host Client inventory, select **Lockdown mode** from the drop-down menu, and select **Enter normal lockdown**.

   A warning message appears.

2. Click **Enter normal lockdown**.

Put an ESXi Host in Strict Lockdown Mode by Using the VMware Host Client

You can use the VMware Host Client to enter strict lockdown mode.

1. Right-click **Host** in the VMware Host Client inventory, select **Lockdown mode** from the drop-down menu, and select **Enter strict lockdown**.

   The warning message appears.

2. Click **Enter strict lockdown**.

Exit Lockdown Mode by Using the VMware Host Client

If you have entered normal or strict lockdown mode on an ESXi host, you can exit lockdown by using the VMware Host Client.

Right-click **Host** in theVMware Host Client inventory, select **Lockdown mode** from the drop-down menu, and select **Exit lockdown**.

Specify Lockdown Mode Exception Users in the VMware Host Client

With vSphere 6.0 and later, you can add users to the exception users list by using the VMware Host Client. These users do not lose their permissions when the host enters lockdown mode. You can add service accounts, such as a backup agent to the exception users list.

Exception users are host local users or Active Directory users with privileges defined locally for the ESXi host. They are not members of an Active Directory group and are not vCenter Server users. These users are allowed to perform operations on the host based on their privileges. That means, for example, that a read-only user cannot disable lockdown mode on a host.

Note: The exception users list is useful for service accounts that perform specific tasks, such as host backups, and not for administrators. Adding administrator users to the exception users list defeats the purpose of lockdown mode.

1. Click **Manage** in the inventory and click **Security & Users**.
2. Click **Lockdown mode**.
3. Click **Add user exception**, enter the name of the user, and click **Add exception**.
4. Optional: Select a name from the exception users list, click **Remove user exception**, and click **Confirm**.

Administering CPU Resources by Using the VMware Host Client

When you connect to an ESXi host with the VMware Host Client, you have access to a limited number of resource management settings.

View Processor Information by Using the VMware Host Client

In the VMware Host Client, you can access information about the current CPU configuration of the ESXi host that you are logged in to.

1. Click **Host** in the VMware Host Client inventory.
2. Expand **Hardware** and expand **CPU**.

   You can view the information about the number and type of physical processors, and the number of logical processors.

Assign a Virtual Machine to a Specific Processor in the VMware Host Client

By using CPU affinity, you can assign a virtual machine to a specific processor. This way, you can assign a virtual machine only to a particular available processor in multiprocessor systems.

Power off the virtual machine.

1. Right-click the virtual machine in the VMware Host Client inventory and select **Edit settings**.
2. Under **Virtual Hardware**, expand **CPU**.
3. Under **Scheduling Affinity**, select physical processor affinity for the virtual machine.
   Use a hyphen to indicate ranges and a comma to separate values.
   For example, `0, 2, 4-7` would indicate processors 0, 2, 4, 5, 6, and 7.
4. Click **Save** to apply your changes.

Monitoring an ESXi Host in the VMware Host Client

When you connect to a host using the VMware Host Client, you can monitor the host health status, and view performance charts, events, tasks, system logs, and notifications.

View Charts in the VMware Host Client

When you are logged in to the VMware Host Client, you can view information about resource usage of the ESXi host that you are managing in line chart form.

To reduce memory consumption, the VMware Host Client only contains statistics for the last hour.

1. Click **Monitor** in the VMware Host Client and click **Performance**.
2. Optional: To view the host usage for the last hour, select an option from the drop-down menu.
   - To view the percentage of CPU that the host used during the last hour, select **CPU**.
   - To view the percentage of memory that the host consumed during the last hour, select **Memory**.
   - To view the percentage of network that the host consumed during the last hour, select **Network**.
   - To view the disk usage that the host consumed during the last hour, select **Disk**.

Monitor Hardware Health Status in the VMware Host Client

When you are logged in to the VMware Host Client, you can monitor the health status of the ESXi host hardware.

Note: Hardware health status is only available when the underlying hardware supports it.

1. Click **Monitor** in the VMware Host Client inventory and click **Hardware**.
2. Select the type of information to view.
3. Optional: Use the filter controls above the list to filter the list.
4. Optional: Click a column heading to sort the list.

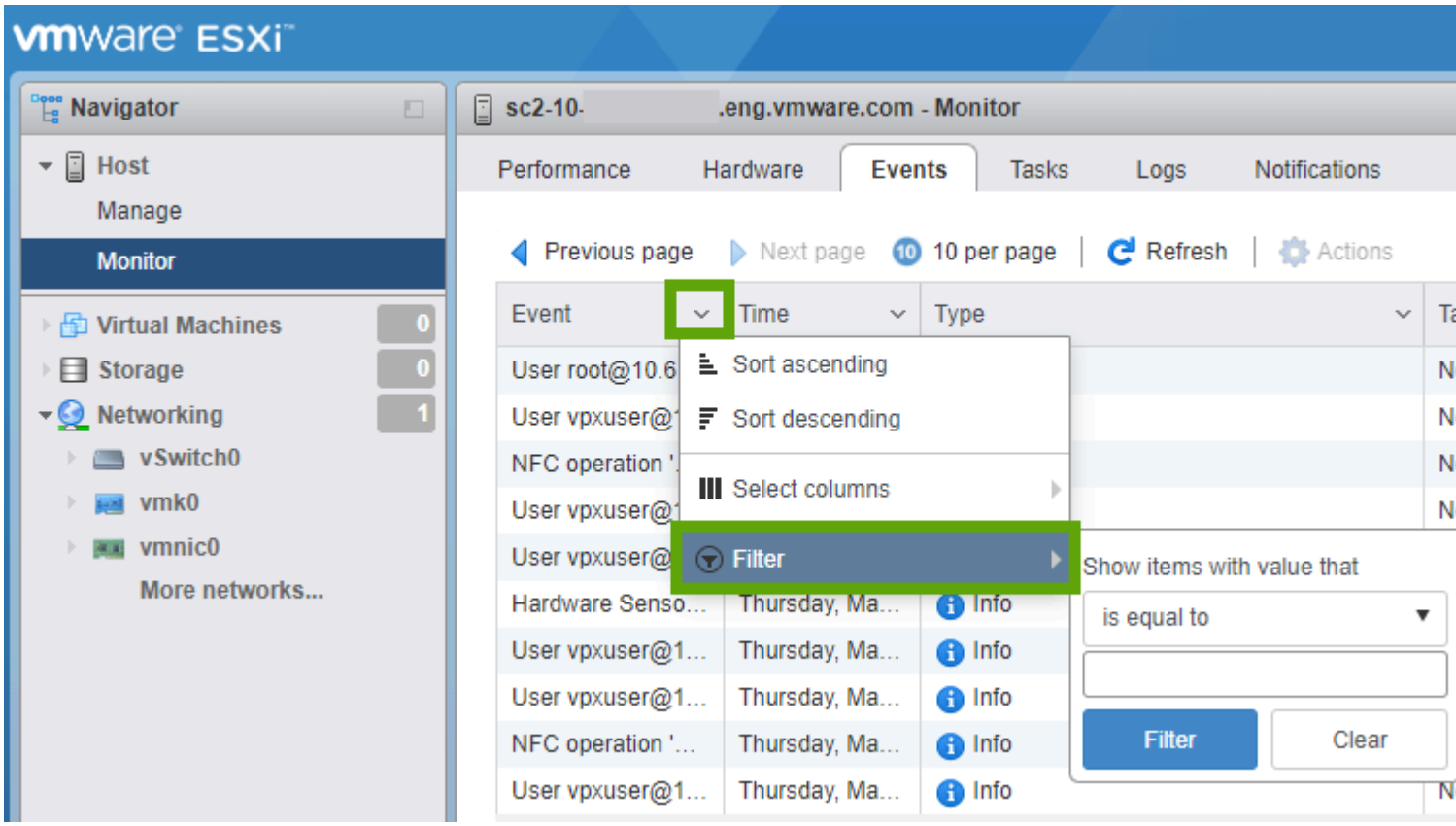
View Events in the VMware Host Client

Events are records of user actions or system actions that occur on an ESXi host. When you are logged in the VMware Host Client, you can view all events associated with the host that you are managing.

Required privilege: **Read-only**.

Click **Monitor** in the VMware Host Client inventory and click **Events**.

a) Optional: Select an event to see event details.
b) Optional: Use the filter controls above the list to filter the list.



c) Optional: Click a column heading to sort the list.

View Tasks in the VMware Host Client

When you are logged in to the VMware Host Client, you can view tasks that are related to the ESXi host. You can view information about task initiator, task state, task result, task description, and so on.

Click **Monitor** in the VMware Host Client inventory and click **Tasks**.

a) Optional: Select a task to see task details.
b) Optional: Use the filter controls above the list to filter the list.
c) Optional: Click a column heading to sort the list.

View System Logs in the VMware Host Client

When you are logged in to an ESXi host with the VMware Host Client, you can view log entries to get information such as who generated an event, when the event was created, and the type of event.

1. Click **Monitor** in the VMware Host Client inventory and click **Logs**.
   The list of logs is displayed.

2. Optional: Click a log to view log details.
3. Optional: Right-click a log and select one of the following options:
   - **Open in new window**
   - **Generate support bundle**

View Notifications in the VMware Host Client

When you are logged in the VMware Host Client, you can view host notifications and recommendations for related tasks that you should perform.

1. Click **Monitor** in the VMware Host Client inventory and click **Notifications**.
2. Select a notification from the list to view the recommended action.

   A message with a recommended action and a description is displayed under the notifications list.

Virtual Machine Management with the VMware Host Client

Virtual machines can be configured like physical computers and can perform the same tasks as physical computers. Virtual machines also support special features that physical computers do not support.

You can use the VMware Host Client to create, register, and manage virtual machines, and to conduct daily administrative and troubleshooting tasks.

Create a Virtual Machine in the VMware Host Client

Virtual machines are the key component in a virtual infrastructure. You can create virtual machines to add to the host inventory. When you create a virtual machine, you associate it with a particular datastore and select an operating system and virtual hardware options. After you power on the virtual machine, it consumes resources dynamically as the workload increases, or returns resources dynamically as the workload decreases.

Verify that you have the **VirtualMachine** > **Inventory** > **Create** privileges.

Depending on the properties of the virtual machine you want to create, you might need the following additional privileges:

- **VirtualMachine** > **Config** > **AddExistingDisk** if including a virtual disk device that refers to an existing virtual disk file (not RDM).
- **VirtualMachine** > **Config** > **AddNewDisk** if including a virtual disk device that creates a new virtual disk file (not RDM).
- **VirtualMachine** > **Config** > **RawDevice** if including a raw device mapping (RDM) or SCSI passthrough device.
- **VirtualMachine** > **Config** > **HostUSBDevice** if including a VirtualUSB device backed by a host USB device.
- **VirtualMachine** > **Config** > **AdvancedConfig** if setting values in `ConfigSpec.extraConfig`.
- **VirtualMachine** > **Config** > **SwapPlacement** if setting swapPlacement.
- **Datastore** > **AllocateSpace** required on all datastores where the virtual machine and its virtual disks are created.
- **Network** > **Assign** required on the network which is assigned to the new virtual machine that is being created.

Every virtual machine has virtual devices that provide the same function as physical hardware. A virtual machine gets CPU and memory, access to storage, and network connectivity from the host it runs on.

1. Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.

   The **New Virtual Machine** wizard opens.

2. Select **Create a new virtual machine** and click **Next**.
3. On the **Select a name and guest OS** page, provide a unique name for the virtual machine and configure the guest operating system.
   a) In the **Name** text box, enter a name for the virtual machine.
   b) From the **Compatibility** drop-down menu, select the virtual machine compatibility.
   c) From the **Guest OS family** drop-down menu, select the guest operating system.
   d) From the **Guest OS version** drop-down menu, select the guest operating system version.
   e) To enable VBS on the virtual machine, select the **Enable Windows Virtualization Based Security** check box and click **Next**.

      Note: The **Enable Windows Virtualization Based Security** option only appears for the latest Windows OS versions, for example, Windows 10 and Windows Server 2016, and if the virtual machine compatibility is ESXi 6.7 and later.

      When you enable this option, hardware virtualization, IOMMU, EFI, and secure boot become available to the guest operating system. You must also enable **Virtualization Based Security** within the guest operating system of this virtual machine.
4. Click **Next**.
5. On the **Select storage** page, select the storage type for the virtual machine and a datastore where to store the virtual machine files.
   a) To save all the virtual machine disks and configuration files on a standard datastore, click the **Standard** button.
   b) To save the virtual machine hard disks on the host-local PMem datastore, click the **Persistent Memory** button.
   c) Select a datastore from the list and click **Next**.

      Note: You cannot store the configuration files on a PMem datastore. If you choose to use PMem, you must select a regular datastore for the configuration files of the virtual machine.
6. On the **Customize settings** page, configure the virtual machine hardware and options and click **Next**.

   For information about virtual machine options and virtual disk configuration, including instructions for adding different types of devices, see *vSphere Virtual Machine Administration*.
   a) On the **Customize settings** page, click **Virtual Hardware** and add a new virtual hardware device.
      - Click the **Add hard disk** icon to add a new virtual hard disk.
        Note: You can add a standard or a persistent memory hard disk to the virtual machine. The persistent memory hard disk is stored on the host-local PMem datastore.
      - Click the **Add network adapter** icon to add a NIC to the virtual machine.
      - Click the **Add other device** icon to choose other type of device to add to the virtual machine.
        Note: If the virtual machine uses PMem storage, the hard disks that are stored on a PMem datastore and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust

the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

b) Optional: To view and configure device settings, expand any device.

Option	Description
CPU	The CPU or processor is the portion of a computer system that carries out the instructions of a computer program and is the primary element carrying out the computer's functions. CPUs contain cores. The number of virtual CPUs that are available to a virtual machine depends on the number of licensed CPUs on the host, and the number of CPUs supported by the guest operating system. To use the VMware multicore virtual CPUs feature, you must comply with the requirements of the guest operating system EULA.
Memory	You can add, change, or configure virtual machine memory resources or options to enhance virtual machine performance. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. The memory resource settings for a virtual machine determine how much of the host's memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine.
Hard disk	You can add large-capacity virtual disks to virtual machines and add more space to existing disks, even when the virtual machine is running. You can set most of the virtual disk parameters during virtual machine creation or after you install the guest operating system.
SCSI controller	Storage controllers appear to a virtual machine as different types of SCSI controllers, including BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual SCSI. You can set the type of SCSI bus sharing for a virtual machine and indicate whether the SCSI bus is shared. Depending on the type of sharing, virtual machines can access the same virtual disk simultaneously on the same server or on any server. You can change the SCSI controller configuration for a virtual machine on an ESXi host only.
SATA controller	If a virtual machine has multiple hard disks or CD/DVD-ROM devices, you can add up to three additional SATA controllers to assign the devices to. When you spread the devices among several controllers, you can improve performance and avoid data traffic congestion. You can also add additional controllers if you exceed the thirty-device limit for a single controller. You can boot virtual machines from SATA controllers and use them for large-capacity virtual hard disks.
Network adapter	When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type. The type of network adapters that are available depend on the following factors: • The virtual machine compatibility, which depends on the host that created or most recently updated it. • Whether the virtual machine compatibility has been updated to the latest version for the current host. • The guest operating system.
CD/DVD drive	You can configure DVD or CD devices to connect to client devices, host devices, or Datastore ISO files.

Option	Description
Video Card	You can select the default settings or specify custom settings. You can specify the number of displays, the total video memory, and enable 3D support for guest operating systems on which VMware supports 3D.
PCI device	You can configure PCI devices on an ESXi host to make them available for passthrough. You can also change the hardware label to restrict the virtual machine placement to specific hardware instances.
Dynamic PCI device	PCI passthrough devices are automatically grouped by their vendor and model name. You can configure the desired devices by the vendor and model name instead of selecting a physical PCI device by the hardware address. You can add all available devices with the same hardware label or with a blank hardware label to a virtual machine. When you power on a virtual machine, specific physical PCI passthrough devices with matching vendor and model names attach to the virtual machine.
Security devices	You can configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines and provide additional security to your workloads. You can enable or disable vSGX when you create a virtual machine or edit an existing virtual machine.

c) Optional: To remove a device, click the delete (⊗) icon next to the device.
   This option appears only for virtual hardware that you can remove safely.
d) Optional: To customize virtual machine options, click the **VM Options** button.

7. On the **Ready to complete** page, review the details and click **Finish**.

Deploying a Virtual Machine from an OVF or OVA File in the VMware Host Client

When you connect to an ESXi host by using the VMware Host Client, you can deploy virtual machines from OVF and VMDK files, and from OVA files.

OVF and OVA Limitations for the VMware Host Client

You can create a virtual machine in the VMware Host Client by using OVF and VMDK files, or OVA files. However, several limitations are applicable to this deployment method.

OVA Limitations

You can upload OVA files by using either a Web browser or a client. The memory requirements are significant and might cause the Web browser to stop responding or make the system unstable. The size of the OVA file that can be uploaded depends on how much memory is available on your system. VMware tests show that Google Chrome can upload OVA files of about 1 gigabyte. Mozilla Firefox can extract larger OVA files, but might become unresponsive.

To deploy a large OVA file, VMware recommends to first extract the OVA on your system by running the command `tar -xvf <file.ova>`. Then you can provide the deployment wizard with the OVF and VMDKs as separate files.

OVF Limitations

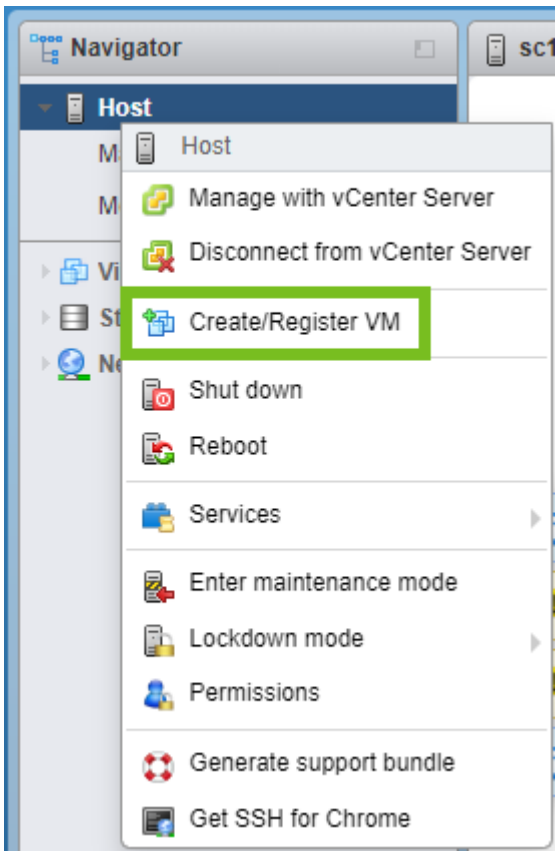
The size of OVF files that a Web browser can upload are also limited. Different Web browsers have different file size limits. Mozilla Firefox has a 4 GB limit. Google Chrome can handle larger files and there is no documented limit.

Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client

Use the **New Virtual Machine** wizard to deploy virtual machines from OVF and VMDK files, or from OVA files.

OVA deployment is limited to files under 1 GB in size due to Web browser limitations. To deploy an OVA file greater than 1 GB, extract the OVA file using tar and provide the OVF and VMDK files separately.

1. Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.



2. On the **Select creation type** page, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
3. On the **Select OVF and VMDK files** page, provide a unique name for the virtual machine.

   Note: Virtual machine names can contain up to 80 characters.
4. To select an OVF and VMDK, or an OVA file to deploy, click the blue pane.

   Your local system storage opens.
5. Select the file that you want to deploy your virtual machine from and click **Open**.

   The file you selected appears in the blue pane.
6. Click **Next**.
7. On the **Select storage** page, select the storage type for the virtual machine.
   a) To save all the virtual machine disks and configuration files on a standard datastore, click the **Standard** button.
   b) To save the virtual machine hard disks on the host-local PMem datastore, click the **Persistent Memory** button.
   c) Select a datastore from the list and click **Next**.

   Important: The configuration files cannot be stored on a PMem datastore. If you choose to use PMem, you must select a regular datastore for the configuration files of the virtual machine.

8. On the **Deployment options** page, select the network mappings, disk provisioning, and whether you want the virtual machine to power on after deployment.
9. Click **Next**.
10. On the **Ready to complete** page, review the details and click **Finish**.

The virtual machine appears in the VMware Host Client inventory under **Virtual Machines**.

Register an Existing Virtual Machine in the VMware Host Client

If you unregister a virtual machine from a host, but you do not delete the virtual machine from the datastore, you can re-register the virtual machine by using the VMware Host Client. Re-registering a virtual machine makes it appear in the inventory.

Use the datastore browser to select either a datastore, a directory, or a `.vmx` file to add to the list of virtual machines that you register. Selecting a datastore or directory searches for all `.vmx` files in that location. You can browse more than once to append virtual machines to the list.

1. Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.
   The **New virtual machine** wizard opens.
2. On the **Select creation type** page, select **Register an existing virtual machine** and click **Next**.
3. On the **Select VMs for registration** page, click **Select one or more virtual machines, a datastore, or a directory**, locate the virtual machine that you want to register, and click **Select**.
4. To remove a virtual machine from the list, select the name of the file and click **Remove selected**.
5. To clear your selection and start again, click **Remove all**.
6. Click **Next**.
7. On the **Ready to complete** page, review the details and click **Finish**.

Using Consoles in the VMware Host Client

You can access a virtual machine through a browser console or through VMware Remote Console (VMRC) in the VMware Host Client and perform different tasks on the virtual machine.

Using Browser Console

Note: The browser console is not supported for any version of ESXi prior to 6.0. You must use VMRC in order to access the browser console.

You can use a browser console to gain access to the guest operating system without installing additional software. For additional console functionalities, such as attaching local hardware, install VMware Remote Console.

Note: Currently browser consoles support only US, Japanese and German keyboard layouts. You must select the desired keyboard layout before opening the console.

Using VMware Remote Console

provides access to virtual machines on remote hosts and performs console and device operations, such as configuring operating system settings and monitoring the virtual machine console for *VMware vSphere*. You can perform a variety of tasks on the virtual machine, such as restarting and shutting down the virtual machine guest operating system, resuming and suspending the virtual machine, configuring VMware Tools updates, configuring and managing the virtual machine and different devices, and so on. VMRC can also modify virtual machine settings such as RAM, CPU cores, and disks. VMware Workstation™, VMware Fusion™ or VMware Player™ work as VMRC clients so you do not need to download and install VMRC if you have any of the three installed on your system.

For a full set of console features, download and install VMRC.

Install the VMware Remote Console Application in the VMware Host Client

The (VMRC) is a standalone console application that enables you to connect to client devices and launch virtual machine consoles on remote hosts.

1. Click **Virtual Machines** in the VMware Host Client inventory.
   The list of virtual machines available on the host is displayed.
2. Select a virtual machine from the list.
3. Click the **Console** toolbar icon and select the **Download VMRC** option.

Launch Remote Console for a Virtual Machine in the VMware Host Client

You can access virtual machines in the VMware Host Client by using . You can launch one or more consoles to access several remote virtual machines at the same time.

Verify that is installed on your local system.

1. Click **Virtual Machines** in the VMware Host Client inventory and select a virtual machine from the list.
2. Click **Console** and select **Launch remote console** from the drop-down menu.
   The opens as a standalone application for the selected virtual machine.

Open a Virtual Machine Console in the VMware Host Client

With the VMware Host Client, you can access the desktop of a virtual machine by launching a console to the virtual machine. From the console, you can perform tasks in the virtual machine, such as configuring operating system settings, running applications, monitoring performance, and so on.

1. Click **Virtual Machines** in the VMware Host Client inventory.
2. Select a powered-on virtual machine from the list.
3. Click the **Console** tool bar icon and select whether to open the console in a pop-up window, new window, or a new tab.

Managing a Guest Operating System in the VMware Host Client

With the VMware Host Client, you can manage the guest operating system of the virtual machine. You can install and upgrade VMware Tools, and you can also shut down, reboot, and change the configured guest operating system.

Shut Down or Restart a Guest Operating System by Using the VMware Host Client

Install VMware Tools on a virtual machine to be able to shut down and restart the guest operating system on that virtual machine.

Click **Virtual Machines** in the VMware Host Client inventory, select a virtual machine, and select your task.

- To shut down a virtual machine, right-click the virtual machine and select **Guest OS** > **Shut down**.
- To restart a virtual machine, right-click the virtual machine and select **Guest OS** > **Restart**.

Change the Guest Operating System in the VMware Host Client

When you change the guest operating system type in the virtual machine settings, you change the setting for the guest operating system in the configuration file of the virtual machine. To change the guest operating system itself, you must install the new operating system in the virtual machine.

Power off the virtual machine.

When you set the guest operating system type for a new virtual machine, vCenter Server applies configuration defaults based on the type of guest operating system. Changing the guest operating system type setting affects the available ranges and recommendations of the virtual machine settings.

1. In the VMware Host Client inventory, right-click the virtual machine and select **Edit Settings**.
2. Click the **VM Options** tab and expand **General Options**.
3. Select a guest operating system type and version.

   If you choose a Windows OS version that supports VBS and if the virtual machine's compatibility is ESXi 6.7 and later, the VBS row appears on the **VM Options** tab.
4. Optional: Click the **Enable Virtualization Based Security** to enable VBS.

   Important: Enabling VBS requires that you use EFI to boot the virtual machine. Changing the firmware might make the guest OS unbootable.
5. Click **Save** to apply your changes.

The virtual machine configuration parameters for the guest operating system are changed. You can now install the guest operating system.

Introduction to VMware Tools

VMware Tools is a set of services and modules that enable several features in VMware products for better management of guests operating systems and seamless user interactions with them.

VMware Tools has the ability to:

- Pass messages from the host operating system to the guest operating system.
- Customize guest operating systems as a part of the vCenter Server and other VMware products.
- Run scripts that help automate guest operating system operations. The scripts run when the power state of the virtual machine changes.
- Synchronize the time in the guest operating system with the time on the host operating system

VMware Tools Lifecycle Management provides a simplified and scalable approach for installation and upgrade of VMware Tools. It includes a number of feature enhancements, driver-related enhancements, and support for new guest operating systems.

You must run the latest version of VMware Tools or use open-vm-tools distributed with the Linux OS distribution. Although a guest operating system can run without VMware Tools, you must always run the latest version of VMware Tools in your guest operating systems to access the latest features and updates.

You can configure your virtual machine to automatically check and apply VMware Tools upgrades each time you power on your virtual machines.

For information about enabling automatic upgrade of VMware Tools on your virtual machines, see *vSphere Virtual Machine Administration Guide*.

Installing VMware Tools

Although you can use guest operating systems without VMware Tools, many VMware features are not available unless you install VMware Tools. VMware Tools enhances the performance of the guest operating system of your virtual machines.

Installing VMware Tools is part of the process of creating new virtual machines. It is important to upgrade VMware Tools as updates become available. For information about creating virtual machines, see the *VMware Tools User Guide*.

The installers for VMware Tools are ISO image files. An ISO image file looks like a CD-ROM to your guest operating system. Each type of guest operating system, including Windows, Linux, Solaris, FreeBSD, and NetWare, has an ISO image file. When you install or upgrade VMware Tools, the first virtual CD-ROM disk drive of the virtual machine temporarily connects to the VMware Tools ISO file of your guest operating system.

For information about installing or upgrading VMware Tools in Windows virtual machines, Linux virtual machines, Mac OS X virtual machines, Solaris virtual machines, NetWare virtual machines, or FreeBSD virtual machines, see the *VMware Tools User Guide*.

Install VMware Tools from the VMware Host Client

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine. VMware Tools enhances the performance and management of the virtual machine.

You can install VMware Tools in one or more virtual machines by using the VMware Host Client.

1. Click **Virtual Machines** in the inventory.
2. Select a virtual machine from the list.

   The virtual machine must be powered on to install VMware Tools.
3. Click **Actions**, select **Guest OS** from the drop-down menu, and select **Install VMware Tools**.

Upgrading VMware Tools

You can upgrade VMware Tools manually or you can configure virtual machines to check for newer versions of VMware Tools and install them.

The guest operating system checks the version of VMware Tools when you power on a virtual machine. The status bar of your virtual machine displays a message when a new version is available.

For vSphere virtual machines, when the installed version of VMware Tools is outdated, the status bar displays the message:

```
A newer version of Tools is available for this VM
```

In Windows virtual machines, you can set VMware Tools to notify you when an upgrade is available. If this notification option is enabled, the VMware Tools icon in the Windows taskbar includes a yellow caution icon when a VMware Tools upgrade is available.

To install a VMware Tools upgrade, you can use the same procedure that you used for installing VMware Tools the first time. Upgrading VMware Tools means installing a new version.

For Windows and Linux guest operating systems, you can configure the virtual machine to automatically upgrade VMware Tools. Although the version check is performed when you power on the virtual machine, in case of Windows guest operating systems, the automatic upgrade occurs when you power off or restart the virtual machine. The status bar displays the message `Installing VMware Tools ...` when an upgrade is in progress. The procedure is mentioned below.

Note:

Upgrading VMware Tools on Windows guest operation systems automatically installs the WDDM graphics drivers. The WDDM graphics driver allows the sleep mode available in guest OS power settings to adjust the sleep options. For example, you can use the sleep mode setting **Change when the computer sleeps** to configure your guest OS to automatically go to sleep mode after a certain time or prevent your guest OS from automatically switching to sleep mode after being idle for some time.

Upgrade VMware Tools in the VMware Host Client

You can upgrade VMware Tools on a virtual machine by using the VMware Host Client.

Power on the virtual machine.

1. Click **Virtual Machines** in the VMware Host Client inventory.
2. Select a virtual machine from the list.
3. Click **Actions**, select **Guest OS** from the drop-down menu, and select **Upgrade VMware Tools**.

Configuring a Virtual Machine in the VMware Host Client

You can add or configure most virtual machine properties during the virtual machine creation process or after you create the virtual machine and install the guest operating system.

You can configure three types of virtual machine properties.

Hardware	View existing hardware configuration and add or remove hardware.
Options	View and configure a number of virtual machine properties such as power management interaction between the guest operating system and the virtual machine, and VMware Tools settings.
Resources	Configure CPUs, CPU hyperthreading sources, memory, and disks.

Check the Virtual Machine Compatibility in the VMware Host Client

You can check the virtual machine compatibility by looking at the virtual machine summary page.

1. Click **Virtual Machines** in the VMware Host Client inventory.
2. Click a virtual machine from the list.
   The virtual machine compatibility appears under the virtual machine name.

Change the Name of a Virtual Machine in the VMware Host Client

You can change the name of a virtual machine after you finish the creation process. Changing the name does not change the name of any virtual machine files or the name of the directory that the files are located in.

Power off the virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Click **VM Options**.
4. In the **VM Name** text box, enter a new name for the virtual machine.
5. Click **Save**.

View the Location of the Virtual Machine Configuration File in the VMware Host Client

You can view the location of the configuration files and the working files of a virtual machine by using the VMware Host Client.

Power off the virtual machine.

This information is useful when you configure backup systems.

1. Click **Virtual Machines** in the inventory.
2. Right-click the virtual machine and click **Edit Settings**.
3. Click the **VM Options** tab and expand **General Options**.
4. Record the location of the configuration files and the working files.
5. Click **Cancel** to exit the screen.

Configure the Virtual Machine Power States in theVMware Host Client

Changing virtual machine power states is useful when you do maintenance on the host. You can use the system default settings for the virtual machine power controls, or you can configure the controls to interact with the guest operating system.

- Verify that you have privileges to perform the intended power operation on the virtual machine.
- To set optional power functions, install VMware Tools on the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

For example, you can configure the **Power off** control to power off the virtual machine or shut down the guest operating system.

You can modify many virtual machine configurations while the virtual machine is running, but you might need to change the virtual machine power state for some configurations.

You cannot configure a **Power on** ( ) action. This action powers on a virtual machine that is stopped, or starts a virtual machine and runs a script if the virtual machine is suspended and VMware Tools is installed and available. If VMware Tools is not installed, it starts the suspended virtual machine and does not run a script.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine from the list and select **Edit settings** from the drop-down menu.
3. On the **VM Options** tab, expand **VMware Tools**.
4. Select an option for the virtual machine **Power off** ( ) control from the drop-down menu.

Option	Description
Power Off	Immediately stops the virtual machine. A Power Off action shuts down the guest operating system or powers off the virtual machine. A message indicates that the guest operating system might not shut down properly. Use this power off option only when necessary.
Shut Down Guest	Uses VMware Tools to initiate an orderly system shut down of the virtual machine. Soft power operations are possible only if the tools are installed in the guest operating system.
System Default	Follows system settings. The current value of the system settings appears in parentheses.

5. Select an option for the **Suspend** ( ) control from the drop-down menu.

Option	Description
Suspend	Pauses all virtual machine activity. When VMware Tools is installed and available, a suspend action runs a script and suspends the virtual machine. If

Option	Description
	VMware Tools is not installed, a Suspend action suspends the virtual machine without running a script.
Put Guest on Standby	Puts the guest operating system on standby. This option stops all processes, but all virtual devices remain connected to the virtual machine.
System Default	Follows system settings. The current value of the system settings appears in parentheses.

6. Select an option for the **Reset** ( ) control from the drop-down menu.

Option	Description
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. If VMware Tools is not installed, a Reset action resets the virtual machine.
Restart Guest	Uses VMware Tools to initiate an orderly restart. Soft power operations are possible only if the tools are installed in the guest operating system.
Default	Follows system settings. The current value of the system settings appears in parentheses.

7. Click **Save**.

Edit the Configuration File Parameters in the VMware Host Client

To fix certain problems with your system, VMware documentation or a VMware Technical Support representative might instruct you to change or add virtual machine configuration parameters.

Power off the virtual machine.

Important: Changing or adding parameters when a system does not have problems might lead to decreased system performance and instability.

The following conditions apply:

- To change a parameter, you must change the existing value for the keyword/value pair. For example, if the existing pair is keyword/value, and you change it to keyword/value2, the new keyword is value2.
- You cannot delete a configuration parameter entry.

CAUTION: You must assign a value to configuration parameter keywords. If you do not assign a value, the keyword might receive a value of 0, false, or disable, which might result in a virtual machine that cannot power on.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **VM Options** tab, expand **Advanced**.
4. In the Configuration Parameters row, click **Edit Configuration**.
   The **Configuration Parameters** dialog box opens.
5. Optional: To add a parameter, click **Add Parameter** and enter a name and value for the parameter.
6. Optional: To change a parameter, type a new value in the **Value** text box for that parameter.
7. Click **OK** to save your changes and exit the **Configuration Parameters** dialog box.

8. Click **Save**.

Configure Autostart Options for a Virtual Machine in the VMware Host Client

You can configure auto start options for a virtual machine to set up the virtual machine to start before or after the other virtual machines on the host.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine from the list.
3. To configure any autostart option, select **Autostart** > **Configure**.
4. To set up the default timing and startup order for virtual machines, select an option from the pop-up menu.

Option	Description
Start delay	Select the time in seconds. After the ESXi host powers on the first virtual machine, the host waits for the specified delay time and powers on the next virtual machine.
Stop delay	Select the time in seconds. Stop delay is the maximum time the ESXi host waits for a shutdown command to complete. The order in which virtual machines are shut down is the reverse of their startup order. After the ESXi host shuts down the first virtual machine within the time you specify, the host shuts down the next virtual machine.
Stop action	From the **Stop action** drop-down menu, select a shut down action that is applicable to the virtual machines on the host when the host shuts down. • **System default** • **Power off** • **Suspend** • **Shut down**
Wait for heartbeat	• Select **Yes** to enable the **Wait for heartbeat** option. You can use this option if the virtual machine has VMware Tools installed. After the ESXi host powers on the first virtual machine, the host immediately powers on the next virtual machine. The startup order in which virtual machines are powered on continues after the virtual machine receives the first heartbeat.

5. Click **Save**.

Upgrade Virtual Machine Compatibility by Using the VMware Host Client

The virtual machine compatibility determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host machine. You can upgrade the compatibility level to make a virtual machine compatible with the latest version of ESXi running on the host.

- Create a backup or snapshot of the virtual machines. See Using Snapshots To Manage Virtual Machines.
- Upgrade VMware Tools. On virtual machines that run Microsoft Windows, if you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machine is stored on VMFS3, VMFS5, or NFS datastores.
- Verify that the compatibility settings for the virtual machines are not set to the latest supported version.

- Determine the ESXi versions that you want the virtual machines to be compatible with. See *vSphere Virtual Machine Administration*.

For information about virtual machine hardware versions and compatibility, see *vSphere Virtual Machine Administration*.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine from the list and select **Upgrade VM Compatibility** from the pop-up menu.
3. Select the latest supported version and click **Upgrade**.

Virtual CPU Configuration

You can add, change, or configure CPU resources to improve virtual machine performance. You can set most of the CPU parameters when you create virtual machines or after the guest operating system is installed. Some actions require that you power off the virtual machine before you change the settings.

VMware uses the following terminology. Understanding these terms can help you plan your strategy for CPU resource allocation.

CPU	The CPU, or processor, is the component of a computer system that performs the tasks required for computer applications to run. The CPU is the primary element that performs the computer functions. CPUs contain cores.
CPU Socket	A CPU socket is a physical connector on a computer motherboard that connects to a single physical CPU. Some motherboards have multiple sockets and can connect multiple multicore processors (CPUs).
Core	A core contains a unit containing an L1 cache and functional units needed to run applications. Cores can independently run applications or threads. One or more cores can exist on a single CPU.
Resource sharing	Shares specify the relative priority or importance of a virtual machine or resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when the two virtual machines are competing for resources.
Resource allocation	You can change CPU resource allocation settings, such as shares, reservation, and limit, when available resource capacity does not meet demands. For example, if at year end, the workload on accounting increases, you can increase the accounting resource pool reserve.
vSphere Virtual Symmetric Multiprocessing (Virtual SMP)	Virtual SMP or vSphere Virtual Symmetric Multiprocessing is a feature that enables a single virtual machine to have multiple processors.

Virtual CPU Limitations

The maximum number of virtual CPUs that you can assign to a virtual machine is 768. The number of virtual CPUs depends on the number of logical CPUs on the host, and the type of guest operating system that is installed on the virtual machine.

Be aware of the following limitations:

- A virtual machine cannot have more virtual CPUs than the number of logical cores on the host. The number of logical cores is equal to the number of physical cores if hyperthreading is deactivated or two times that number if hyperthreading is activated.

- If a running virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a running virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.
- The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.
- Not every guest operating system supports Virtual SMP, and guest operating systems that support this functionality might support fewer processors than are available on the host. For information about Virtual SMP support, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Configuring Multicore Virtual CPUs

VMware multicore virtual CPU support lets you control the number of cores per virtual socket in a virtual machine. This capability lets operating systems with socket restrictions use more of the host CPU cores, which increases overall performance.

Important: When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Using multicore virtual CPUs can be useful when you run operating systems or applications that can take advantage of only a limited number of CPU sockets.

You can configure a virtual machine with ESXi 7.0 Update 1 and later compatibility to have up to 768 virtual CPUs. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical CPUs means the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 virtual CPUs.

You configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single-core CPU, dual-core CPU, tri-core CPU, and so on. Your selection determines the number of sockets that the virtual machine has.

The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

For more information about multicore CPUs, see the *vSphere Resource Management* documentation.

Change the Number of Virtual CPUs

A virtual machine with ESXi 7.0 Update 1 and later compatibility can have up to 768 virtual CPUs. You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hot add is enabled, you can increase the number of virtual CPUs while the virtual machine is running.

- If CPU hot add is not enabled, power off the virtual machine before adding virtual CPUs.
- To hot add multicore CPUs, verify that the virtual machine is compatible with ESXi 5.0 and later.
- Verify that you have the **Virtual Machine** > **Configuration** > **Change CPU Count** privilege.

Virtual CPU hot add is supported for virtual machines with multicore CPU support and ESXi 5.0 and later compatibility. When the virtual machine is powered on and CPU hot add is enabled, you can hot add virtual CPUs to the running virtual machine. You can add only multiples of the number of cores per socket.

If a virtual machine has 128 virtual CPUs or less, you cannot use hot adding to further increase the number of virtual CPUs. To change the number of virtual CPUs beyond that limit, you must first power off the virtual machine. By contrast, if a virtual machine already has more than 128 virtual CPUs, you can use hot adding to further increase the number of virtual CPUs to up to 768.

The maximum number of virtual CPU sockets that a virtual machine can have is 128. If you want to configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

Important: When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **CPU**.
3. From the **CPU** drop-down menu, select the number of cores.
4. From the **Cores Per Socket** drop-down menu, select the number of cores per socket and click **OK**.

Allocate CPU Resources in the VMware Host Client

To manage workload demands, you can change the amount of CPU resources allocated to a virtual machine by using the shares, reservations, and limits settings.

Power off the virtual machine.

A virtual machine has the following user-defined settings that affect its CPU resource allocation.

Limit	Places a limit on the consumption of CPU time for a virtual machine. This value is expressed in MHz or GHz.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in MHz or GHz.
Shares	Each virtual machine is granted CPU shares. The more shares a virtual machine has, the more often it receives a time slice of a CPU when there is no CPU idle time. Shares represent a relative metric for allocating CPU capacity.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, expand **CPU**, and allocate CPU capacity for the virtual machine.

Option	Description
Reservation	Guaranteed CPU allocation for this virtual machine.
Limit	Upper limit for this virtual machine's CPU allocation. Select **Unlimited** to specify no upper limit.
Shares	CPU shares for this virtual machine in relation to the parent's total. Sibling virtual machines share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each virtual machine a specific number of shares, which express a proportional weight.

4. Click **Save**.

Virtual Memory Configuration

You can add, change, or configure virtual machine memory resources or options to enhance virtual machine performance. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. Some actions require that you power off the virtual machine before changing the settings.

The memory resource settings for a virtual machine determine how much of the host's memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size. ESXi hosts limit the memory resource use to the maximum amount useful for the virtual machine, so that you can accept the default of Unlimited memory resources.

Change the Memory Configuration

You can reconfigure the amount of memory allocated to a virtual machine to enhance performance.

Verify that you have the **Virtual machine** > **Configuration** > **Change Memory** privilege on the virtual machine.

Minimum memory size is 4 MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96 MB of RAM or they cannot power on.

Maximum memory size for virtual machines that use BIOS firmware is 24560 GB. You must use EFI firmware for virtual machines with memory size greater than 6128 GB.

Maximum memory size for a virtual machine depends on the physical memory of the ESXi host and the virtual machine compatibility settings.

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance. The maximum for best performance represents the threshold above which the physical memory of the ESXi host is insufficient to run the virtual machine at full speed. This value fluctuates as conditions on the host change, for example, as virtual machines are powered on or off.

The memory size must be a multiple of 4 MB.

Table 525: Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 7.0 Update 3	ESXi 7.0 Update 3 and later	24560 GB
ESXi 7.0 Update 2	ESXi 7.0 Update 2 and later	24560 GB
ESXi 7.0 Update 1	ESXi 7.0 Update 1 and later	24560 GB
ESXi 7.0	ESXi 7.0 and later	6128 GB
ESXi 6.7 Update 2	ESXi 6.7 Update 2 and later	6128 GB
ESXi 6.7	ESXi 6.7 and later	6128 GB
ESXi 6.5	ESXi 6.5 and later	6128 GB
ESXi 6.0	ESXi 6.0 and later	4080 GB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a virtual machine with ESXi 6.0 and later compatibility running on ESXi 6.5 is restricted to 4080 GB.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Memory** and change the memory configuration.
   a) In the **Memory** text box, enter the amount of RAM to assign to the virtual machine.
   b) Select whether the memory is specified in MB, GB or TB.
3. Click **OK**.

Allocate Memory Resources

You can change the amount of memory resources allocated to a virtual machine by using the shares, reservations, and limits settings. The host determines the appropriate amount of physical RAM to allocate to virtual machines based on these settings. You can assign a high or low shares value to a virtual machine, depending on its load and status.

Verify that the virtual machine is turned off.

The following user-defined settings affect the memory resource allocation of a virtual machine.

Limit	Places a limit on the consumption of memory for a virtual machine. This value is expressed in megabytes.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in megabytes. If the reservation cannot be met, the virtual machine will not turn on.
Shares	Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the greater share of host memory it receives. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the *vSphere Resource Management* documentation.

You cannot assign a reservation to a virtual machine that is larger than its configured memory. If you give a virtual machine a large reservation and reduce its configured memory size, the reservation is reduced to match the new configured memory size.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand Memory, and allocate the memory capacity for the virtual machine.

Option	Description
Reservation	Guaranteed memory allocation for this virtual machine.
Limit	Upper limit for this virtual machine's memory allocation. Select **Unlimited** to specify no upper limit.
Shares	The values **Low**, **Normal**, **High**, and **Custom** are compared to the sum of all shares of all virtual machines on the server.

3. Click **OK**.

Change Memory Hot Add Settings

Memory hot add lets you add memory resources for a virtual machine while that virtual machine is powered on.

- Power off the virtual machine.
- Verify that the virtual machine has a guest operating system that supports memory hot add functionality.
- Verify that the virtual machine compatibility is ESXi 4.x and later.

- Verify that VMware Tools is installed.

Enabling memory hot add produces some memory overhead on the ESXi host for the virtual machine.

Note: If the ESXi host is of version 7.0 Update 2 and earlier, hot-adding memory to a virtual machine with NVIDIA vGPU requires that the ESXi host has a free vGPU slot. Starting with vSphere 7.0 Update 3, the source host does not require to have a free vGPU slot.

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Memory**, and select **Enable** to enable adding memory to the virtual machine while it is powered on.
3. Click **OK**.

You can now add memory to a virtual machine, even if the virtual machine is turned on.

Add an NVDIMM device to a VM in the VMware Host Client

Add a virtual NVDIMM device to a virtual machine to enable it to use non-volatile, or persistent, computer memory. Non-volatile memory (NVM), or persistent memory (PMem), combines the high data transfer rates of the volatile memory with the persistence and resiliency of traditional storage. The virtual NVDIMM device is a virtual NVM device that can retain stored data through reboots or power source failures.

- Verify that the guest OS of the virtual machine supports PMem.
- Verify that the virtual hardware version is 14 or later.
- Verify that you have the **Datastore** > **Allocate space** privilege.
- Verify that the host or the cluster on which the virtual machine resides has available PMem resources.

Virtual machines consume the PMem resource of the host through a virtual non-volatile dual in-line memory module (NVDIMM) or through a virtual persistent memory disk.

For more information about persistent memory, see Managing Persistent Memory

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Under the **Virtual Hardware** tab, click **Add other device** and select **NVDIMM** from the drop-down menu.

   The NVDIMM device appears in the Virtual Hardware devices list. Each virtual machine can have a maximum of 64 NVDIMM devices.
4. Configure the newly added NVDIMM device.
   a) In the Virtual Hardware devices list, expand **New NVDIMM**.
   b) Enter the size of the new NVDIMM device.

      Note: You can change the size of the NVDIMM device at a later time. The virtual machine must be powered off.
   c) Select the NVDIMM controller location or leave the default one.
5. Click **Save** to close the wizard.

Network Virtual Machine Configuration

ESXi networking features enable communication between virtual machines on the same host, between virtual machines on different hosts, and between other virtual and physical machines.

The networking features also allow management of ESXi hosts and enable communication between VMkernel services, such as NFS, iSCSI, or vSphere vMotion, and the physical network. When you configure networking for a virtual machine, you select or change an adapter type, a network connection, and whether to connect the network when the virtual machine powers on.

Network Adapter Basics

When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.

Network Adapter Types

The type of network adapters that are available depend on the following factors:

- The virtual machine compatibility, which depends on the host that created or most recently updated it.
- Whether the virtual machine compatibility has been updated to the latest version for the current host.
- The guest operating system.

Supported NICs currently differ between an on-premises environment and VMware Cloud on AWS. The following NIC types are supported in an on-premises deployment:

E1000E	Emulated version of the Intel 82574 Gigabit Ethernet NIC. E1000E is the default adapter for Windows 8 and Windows Server 2012.
E1000	Emulated version of the Intel 82545EM Gigabit Ethernet NIC, with drivers available in most newer guest operating systems, including Windows XP and later and Linux versions 2.4.19 and later.
Flexible	Identifies itself as a Vlance adapter when a virtual machine boots, but initializes itself and functions as either a Vlance or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlance adapter to the higher performance VMXNET adapter.
Vlance	Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in 32-bit legacy guest operating systems. A virtual machine configured with this network adapter can use its network immediately.
VMXNET	Optimized for performance in a virtual machine and has no physical counterpart. Because operating system vendors do not provide built-in drivers for this card, you must install VMware Tools to have a driver for the VMXNET network adapter available.
VMXNET 2 (Enhanced)	Based on the VMXNET adapter but provides high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads. VMXNET 2 (Enhanced) is available only for some guest operating systems on ESX/ ESXi 3.5 and later.
VMXNET 3	A paravirtualized NIC designed for performance. VMXNET 3 offers all the features available in VMXNET 2 and adds several new features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2.
PVRDMA	A paravirtualized NIC that supports remote direct memory access (RDMA) between virtual machines through the OFED verbs API. All virtual machines must have a PVRDMA device and should be connected to a distributed switch. PVRDMA supports VMware vSphere vMotion and snapshot technology. It is available in virtual machines with hardware version 13 and guest operating system Linux kernel 4.6 and later. For information about assigning an PVRDMA network adapter to a virtual machine, see the *vSphere Networking* documentation.
SR-IOV passthrough	Representation of a virtual function (VF) on a physical NIC with SR-IOV support. The virtual machine and the physical adapter

exchange data without using the VMkernel as an intermediary. This adapter type is suitable for virtual machines where latency might cause failure or that require more CPU resources.

SR-IOV passthrough is available in ESXi 6.0 and later for guest operating systems Red Hat Enterprise Linux 6 and later, and Windows Server 2008 R2 with SP2. An operating system release might contain a default VF driver for certain NICs, while for others you must download and install it from a location provided by the vendor of the NIC or of the host.

For information about assigning an SR-IOV passthrough network adapter to a virtual machine, see the *vSphere Networking* documentation.

For network adapter compatibility considerations, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Legacy Network Adapters and ESXi Virtual Hardware Versions

The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to use a virtual hardware version, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Network Adapters and Legacy Virtual Machines

Legacy virtual machines are virtual machines that are supported by the product in use, but are not current for that product. The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to correspond with an upgrade to a newer version of an ESXi host, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Change the Configuration of the Virtual Network Adapter in theVMware Host Client

You can configure the power-on connection setting, the MAC address, and the network connection of the virtual network adapter of a virtual machine.

Required privileges:

- **Virtual Machine** > **Configuration** > **Modify device settings** for editing the MAC address and network.

- **Virtual Machine** > **Interaction** > **Device connection** for changing **Connect** and **Connect at power on**.
- **Network** > **Assign network**

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Click the **Virtual Hardware** tab and select the appropriate Network Adapter (NIC) from the hardware list.
4. Optional: To connect the virtual NIC when the virtual machine is powered on, select **Connect at power on**.
5. Optional: Select the adapter type from the **Adapter Type** drop-down menu.
6. Select an option for MAC address configuration.

Option	Description
Automatic	vSphere assigns a MAC address automatically.
Manual	Enter the MAC address to use.

7. Click **Save**.

Add a Network Adapter to a Virtual Machine in the VMware Host Client

When you add a network adapter (NIC) to a virtual machine, you must select the adapter type, the network connection, and whether the device connects when the virtual machine is powered on.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Click the **Virtual Hardware** tab and click **Add network adapter**.
4. In the network connection panel, select either a network with a specific label or a legacy network.
5. Optional: To configure the virtual NIC to connect when the virtual machine is powered on, select **Connect at power on**.
6. Click **Save**.

Virtual Disk Configuration

You can add large-capacity virtual disks to virtual machines and add more space to existing disks, even when the virtual machine is running. You can set most of the virtual disk parameters during virtual machine creation or after you install the guest operating system.

You can store virtual machine data in a new virtual disk, an existing virtual disk, or a mapped SAN LUN. A virtual disk appears as a single hard disk to the guest operating system. The virtual disk is composed of one or more files on the host file system. You can copy or move virtual disks on the same hosts or between hosts.

For virtual machines running on an ESXi host, you can store virtual machine data directly on a SAN LUN instead of using a virtual disk file. This option is useful if in your virtual machines you run applications that must detect the physical characteristics of the storage device. Mapping a SAN LUN also allows you to use existing SAN commands to manage storage for the disk.

When you map a LUN to a VMFS volume, vCenter Server or the ESXi host creates a raw device mapping (RDM) file that points to the raw LUN. Encapsulating disk information in a file allows vCenter Server or the ESXi host to lock the LUN so that only one virtual machine can write to it. This file has a `.vmdk` extension, but the file contains only disk information that describes the mapping to the LUN on the ESXi system. The actual data is stored on the LUN. You cannot deploy a virtual machine from a template and store its data on a LUN. You can store its data only in a virtual disk file.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

About Virtual Disk Provisioning Policies

When you perform certain virtual machine management operations, you can specify a provisioning policy for the virtual disk file. The operations include creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine.

NFS datastores with Hardware Acceleration and VMFS datastores support the following disk provisioning policies. On NFS datastores that do not support Hardware Acceleration, only thin format is available.

You can use Storage vMotion or cross-host Storage vMotion to transform virtual disks from one format to another.

Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand later on first write from the virtual machine. Virtual machines do not read stale data from the physical device.
Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks. Increasing the size of an Eager Zeroed Thick virtual disk causes a significant stun time for the virtual machine.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed. **Note:** If a virtual disk supports clustering solutions such as Fault Tolerance, do not make the disk thin.

Change the Virtual Disk Configuration in theVMware Host Client

If you run out of disk space, you can increase the size of the disk. You can change the virtual device node and the persistence mode of virtual disk configuration of a virtual machine.

Power off the virtual machine.

Verify that you have the following privileges:

- **Virtual machine** > **Configuration** > **Modify device settings** on the virtual machine.
- **Virtual machine** > **Configuration** > **Extend virtual disk** on the virtual machine.
- **Datastore** > **Allocate space** on the datastore.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, expand the hard disk to view all disk options.
4. Optional: To change the size of the disk, enter a new value in the text box and select the units from the drop-down menu.
5. Optional: To change the way that disks are affected by snapshots, select a disk mode from the **Disk Mode** drop-down menu.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent-Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent-Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset the virtual machine.

6. Click **Save**.

Add a New Standard Hard Disk to a Virtual Machine in theVMware Host Client

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

- Verify that you are familiar with configuration options and caveats for adding virtual hard disks. See Virtual Disk Configuration.
- Before you add disks larger than 2TB in size to a virtual machine, see *vSphere Virtual Machine Administration*.
- Verify that you have the**Virtual machine** > **Configuration** > **Add new disk** privilege on the destination folder or datastore.

Power off the virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Optional: To delete an existing hard disk, move your pointer over the disk and click the **Remove** icon (**X**).

   The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.
4. On the **Virtual Hardware** tab, select **Add hard disk** and select **New standard hard disk** from the drop-down menu.

   The hard disk appears in the Virtual Hardware devices list.

5. Expand **New Hard disk**.
6. Optional: Enter a value for the hard disk size and select the units from the drop-down menu.
7. Select the datastore location where you want to store the virtual machine files.
8. Select the format for the virtual machine disk.

Option	Description
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out during creation. It might take much longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially requires. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

9. In the **Shares** drop-down menu, select a value for the shares to allocate to the virtual disk.

   Shares is a value that represents the relative metric for controlling disk bandwidth. The values Low, Normal, High, and Custom are compared to the sum of all shares of all virtual machines on the host.
10. If you selected **Custom**, enter a number of shares in the text box.
11. In the **Limit IOPs** box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.

    This value is the upper limit of I/O operations per second allocated to the virtual disk.
12. Accept the default or select a different virtual device node.

    In most cases, you can accept the default device node. For a hard disk, using a nondefault device node makes controlling the boot order or having different SCSI controller types easier. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine that is using a Buslogic controller with bus sharing turned on.
13. Optional: Select a disk mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent-Persistent	Disks in persistent mode behave like conventional physical computer disks. All data written to a disk in persistent mode are written permanently to the disk.
Independent-Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. The virtual disk returns to the same state every time you restart the virtual machine. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

14. Click **Save**.

Add an Existing Hard Disk to a Virtual Machine in the VMware Host Client

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

- Verify that you are familiar with controller and virtual device node behavior for different virtual hard disk configurations.
- Verify that you have the **Virtual machine** > **Configuration** > **Add existing disk** privilege on the destination folder or datastore.

Power off the virtual machine.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an existing hard disk at the end of the creation process.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add hard disk** and select **Existing hard disk** from the drop-down menu.
4. Optional: To delete an existing hard disk, move your pointer over the disk and click the **Remove** icon (**X**).
   The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.
5. In the Datastore column, expand a datastore, select a virtual machine folder, and select the disk to add.
   The disk file appears in the Contents column. The **File type** menu shows the compatibility file types for this disk.
6. Click **Select** and click **Save** to add the existing hard disk.

Add a Persistent Memory Disk in the Host Client

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

- Verify that you are familiar with configuration options and caveats for adding virtual hard disks. See Virtual Disk Configuration.
- Before you add disks larger than 2TB in size to a virtual machine, see *vSphere Virtual Machine Administration*.
- Verify that you have the **Virtual machine** > **Configuration** > **Add new disk** privilege on the destination folder or datastore.

Power off the virtual machine.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an existing hard disk at the end of the creation process.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add hard disk** and select **New persistent memory disk** from the drop-down menu.
   The hard disk appears in the Virtual Hardware devices list. By default, the disk is stored on the host-local PMem datastore and you cannot change the datastore.

4. Optional: Configure the settings for the new hard disk and click **Save** to close the wizard.
   a) Expand **New Hard disk**.
   b) Enter a value for the hard disk size and select the units from the drop-down menu.

      Note: All persistent memory hard disks and NVDIMM modules that you add to the virtual machine share the same PMem resources. So, you must adjust the size of the newly added persistent memory devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.
   c) From the **Shares** drop-down menu, select a value for the shares to allocate to the virtual disk.

      Shares is a value that represents the relative metric for controlling disk bandwidth. The values Low, Normal, High, and Custom are compared to the sum of all shares of all virtual machines on the host.
   d) From the **Controller location** drop-down menu, select the location of the controller that the new hard disk uses.
   e) Select a disk mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent-Persistent	Disks in persistent mode behave like conventional physical computer disks. All data written to a disk in persistent mode are written permanently to the disk.
Independent-Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. The virtual disk returns to the same state every time you restart the virtual machine. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

Use Disk Shares to Prioritize Virtual Machines in the VMware Host Client

You can change the disk resources for a virtual machine. If multiple virtual machines access the same VMFS datastore and the same logical unit number (LUN), use disk shares to prioritize the level of access that virtual machines have to resources. Disk shares distinguish high-priority from low-priority virtual machines.

Power off the virtual machine.

You can allocate the I/O bandwidth of the host to the virtual hard disks of a virtual machine. You cannot pool disk I/O across a cluster.

The shares value represents the relative metric for controlling disk bandwidth to all virtual machines.

Disk shares are relevant only within a given host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.

You can select an IOP limit, which sets an upper limit for storage resources that are allocated to a virtual machine. IOPs are the number of I/O operations per second.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, expand the hard disk to view the disk options.
4. In the **Shares** drop-down menu, select a value for the shares to allocate to the virtual machine.
5. If you selected **Custom**, enter a number of shares in the text box.
6. In the **Limit - IOPs** text box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.
7. Click **Save**.

Virtual Machine Controller Configuration in the VMware Host Client

In the VMware Host Client, you can add various controllers to virtual machines, such as USB controllers, SCSI controllers, Paravirtual SCSI controllers, and SATA controllers. You can also change the SCSI Bus sharing configuration and the SCSI controller type.

Add a USB Controller to a Virtual Machine

To support USB passthrough from an ESXi host or from a client computer to a virtual machine, you can add a USB controller to the virtual machine.

- Verify that the ESXi hosts have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices.
- Verify that the client computers have USB controller hardware and modules that support USB 3.1, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, verify that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine** > **Configuration** > **Add or Remove Device**

In the vSphere Client, you can add one xHCI controller and one EHCI+UHCI controller. From hardware version 11 to hardware version 16, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeed ports and four logical USB 2.0 ports). With hardware version 17, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.1 SuperSpeedPlus ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 526: USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to a VM	Supported for Passthrough from Client Computer to a VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.1, 2.0, and 1.1	Yes USB 3.1, 2.0, and 1.1 devices only.	Yes Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for access to a USB mouse and keyboard.

For virtual machines with Windows or Linux guest operating systems, you can add one or two controllers of different types. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes more than 15 controllers and you connect USB devices to them, the devices are not available to the virtual machine.

1. Right-click a virtual machine from the vSphere inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, click **Add New Device** and from the drop-down menu select **USB Controller**.
   The controller appears in the **Virtual Hardware** devices list.
3. To change the USB controller type, expand **New USB Controller**.
4. Click **OK**.

Add one or more USB devices to the virtual machine.

Add SCSI Controllers in the VMware Host Client

You can add SCSI controllers to an existing virtual machine by adding hard disks on unused SCSI Bus numbers.

Power off the virtual machine.

Adding a new hard disk on an unused SCSI Bus number creates a new SCSI controller.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add hard disk** and select **New hard disk** from the drop-down menu.
4. Expand the hard disk to view all options.
5. In the **Controller location** section, select an unused SCSI Bus number from the drop-down menu.
   For example, bus and device numbers 0:0 - 0:15 are used by the initial SCSI controller. The second SCSI controller uses bus and device numbers 1:0 - 1:15.
6. Click **Save**.

The new hard disk and new SCSI controller are simultaneously created.

Change the SCSI Bus Sharing Configuration in theVMware Host Client

You can set the type of SCSI bus sharing for a virtual machine and indicate whether to share the SCSI bus. Depending on the type of sharing, virtual machines can access the same virtual disk simultaneously on the same server or on any server.

Power off the virtual machine.

You can change the SCSI controller configuration for a virtual machine only if the virtual machine is on anESXi host.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, expand the SCSI Controller that you want to edit.
4. Select the type of sharing in the **SCSI Bus Sharing** list.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.

Option	Description
Virtual	Virtual disks can be shared by virtual machines on the same server.
Physical	Virtual disks can be shared by virtual machines on any server.

5. Click **Save**.

Change the SCSI Controller Type in the VMware Host Client

You can attach virtual disks and RDMs to virtual machines by configuring virtual SCSI controller on the virtual machines.

Power off the virtual machine.

The choice of SCSI controller does not affect whether your virtual disk is an IDE or SCSI disk. The IDE adapter is always ATAPI. The default for your guest operating system is already selected. Older guest operating systems have BusLogic adapter as their default controller.

If you create an LSI Logic virtual machine and add a virtual disk that uses BusLogic adapters, the virtual machine boots from the BusLogic adapters disk. LSI Logic SAS is available only for virtual machines with hardware version 7 or later. Disks with snapshots might not experience performance gains when used on LSI Logic SAS, VMware Paravirtual, and LSI Logic Parallel adapters.

CAUTION: Changing the SCSI controller type might result in a virtual machine boot failure.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Click the **Virtual Hardware** tab and expand a SCSI controller.
4. Select a SCSI controller type from the drop-down menu.
5. Click **Save**.

About VMware Paravirtual SCSI Controllers

VMware Paravirtual SCSI controllers are high performance storage controllers that can result in greater throughput and lower CPU use. These controllers are best suited for high performance storage environments.

VMware Paravirtual SCSI controllers are available for virtual machines with ESXi 4.x and later compatibility. Disks on such controllers might not experience optimal performance gains if they have snapshots or if memory on the ESXi host is over committed. This behavior does not mitigate the overall performance gain of using VMware Paravirtual SCSI controllers as compared to other SCSI controller options.

For platform support for VMware Paravirtual SCSI controllers, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Add a Paravirtual SCSI Controller in the VMware Host Client

You can add a VMware Paravirtual SCSI high performance storage controller to provide greater throughput and lower CPU utilization.

- Verify that the virtual machine has a guest operating system with VMware Tools installed.
- Verify that the virtual machine has hardware version 7 or later.
- Familiarize yourself with VMware Paravirtual SCSI limitations. See *vSphere Virtual Machine Administration*.
- To access boot disk devices attached to a VMware Paravirtual SCSI controller, verify that the virtual machine has a Windows 2003 or Windows 2008 guest operating system.

- In some operating systems, before you change the controller type you must create a virtual machine with an LSI Logic controller and install VMware Tools.

Power off the virtual machine.

VMware Paravirtual SCSI controllers are best suited for environments, especially SAN environments, that run I/O-intensive applications.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, click **Add other device** and select **SCSI Controller** from the drop-down menu.
   The new SCSI Controllers appear in the Hardware list.
4. Click the **New SCSI Controller** and select **VMware Paravirtual** from the drop-down menu.
5. Click **Save**.

Add a SATA Controller to a Virtual Machine in the VMware Host Client

If a virtual machine has multiple hard disks or CD/DVD-ROM devices, you can add up to three additional SATA controllers to assign the devices to. When you assign the devices to different controllers, you can improve performance and avoid data traffic congestion. You can also add controllers if you need to exceed the thirty-device limit for a single controller.

- Verify that the virtual machine compatibility is ESXi 5.5 and later.
- Verify that you are familiar with storage controller behavior and limitations. See *vSphere Virtual Machine Administration*.
- Verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.
- Power off the virtual machine.

You can boot virtual machines from SATA controllers and use them for large-capacity virtual hard disks.

Not all guest operating systems support AHCI SATA controllers. Typically, when you create virtual machines with ESXi 5.5 and later compatibility and Mac OS X guest operating systems, a SATA controller is added by default for the virtual hard disk and CD/DVD-ROM devices. Most guest operating systems, including Windows Vista and later, have a default SATA controller for CD/DVD-ROM devices. For verification, see the appropriate *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device**, and select **SATA Controller** from the drop-down menu.
   The SATA controller appears in the hardware list.
4. Click **Save**.

Add an NVMe Controller in the VMware Host Client

If a virtual machine has multiple hard disks, you can add up to four virtual NVMe controllers to which to assign the disks. Using a NVMe controller significantly reduces the software overhead for processing guest OS I/O, as compared to AHCI SATA or SCSI controllers.

- Verify that the virtual machine has a guest operating system that supports NVMe.
- Verify that the virtual machine compatibility is ESXi 6.5 or later.
- Verify that you are familiar with storage controllers behavior and limitations. For more information, see the *Virtual Machine Administration* guide.

- Verify that you have the **Virtual machine** > **Configuration** > **Add new disk** privilege on the virtual machine.

NVMe controllers perform best with virtual disks on an all-flash disk array, local NVMe SSD, and PMem storage.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. Under the **Virtual Hardware** tab, click the **Add other device** icon and select **NVMe controller** from the drop-down menu.

A new NVMe controller is added to the virtual machine.

You can add a hard disk to the virtual machine and assign it to the NVMe controller.

Other Virtual Machine Device Configuration in the VMware Host Client

In addition to configuring virtual machine CPU and Memory, and adding hard disks and virtual network adapters, you can also add and configure virtual hardware, such as DVD/CD-ROM drives, floppy drives, and SCSI devices. You can also add a virtual Watchdog Timer (VWDT) device, Precision Clock device, and PCI devices.

Add a CD or DVD Drive to a Virtual Machine in theVMware Host Client

You can use a physical drive on a client or host, or you can use an ISO image to add a CD/DVD drive to a virtual machine.

Power off the virtual machine.

If you want to add a CD/DVD drive that is backed up by USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding or removing SCSI devices from anESXi host is not supported.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **CD/DVD Drive** from the drop-down menu.
4. Expand **CD/DVD drive** and select an option.

Option	Description
Use physical drive	1. Select **Client Device** as the location. 2. From the **Device Mode** drop-down menu, select **Emulate CD-ROM** or **Passthrough CD-ROM**.
Use ISO Image	1. Select **Datastore ISO File** as the location. 2. Enter the path and filename for the image file, or click **Browse** to navigate to the file.

5. If you do not want the CD-ROM drive to connect when the virtual machine starts, deselect **Connect at power on**.
6. Select the virtual device node that the drive uses in the virtual machine.
7. Click **Save**.

Add a Floppy Drive to a Virtual Machine in theVMware Host Client

Use a physical floppy drive or a floppy image to add a floppy drive to a virtual machine.

- Power off the virtual machine.

- Verify that you have the**Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.

ESXi does not support floppy drives that are backed up by a physical floppy drive on the host.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **Floppy Drive** from the drop-down menu.
   The Floppy drive appears in the hardware list.
4. Expand **Floppy drive** and select the type of device you want to use.

Option	Description
Client Device	Select this option to connect the floppy device to a physical floppy device or a `.flp` floppy image on the system from which you access theVMware Host Client.
Use existing floppy image	1. Select this option to connect the virtual device to an existing image of a floppy drive on a datastore accessible to the host. 2. Click **Browse** and select the floppy image.

5. Optional: Select **Connect at power on** to configure the device to connect when the virtual machine powers on.
6. Click **Save**.

Add a USB Device to a Virtual Machine in the VMware Host Client

By using the VMware Host Client, you can add a USB device to a virtual machine.

- Verify that a USB controller is present. See Add a USB Controller to a Virtual Machine.
- Add a physical USB device to the ESXi host where the virtual machine is located by plugging the USB device into the host.

Note: If the ESXi host does not have available USB devices, you cannot add a USB device to the virtual machine.

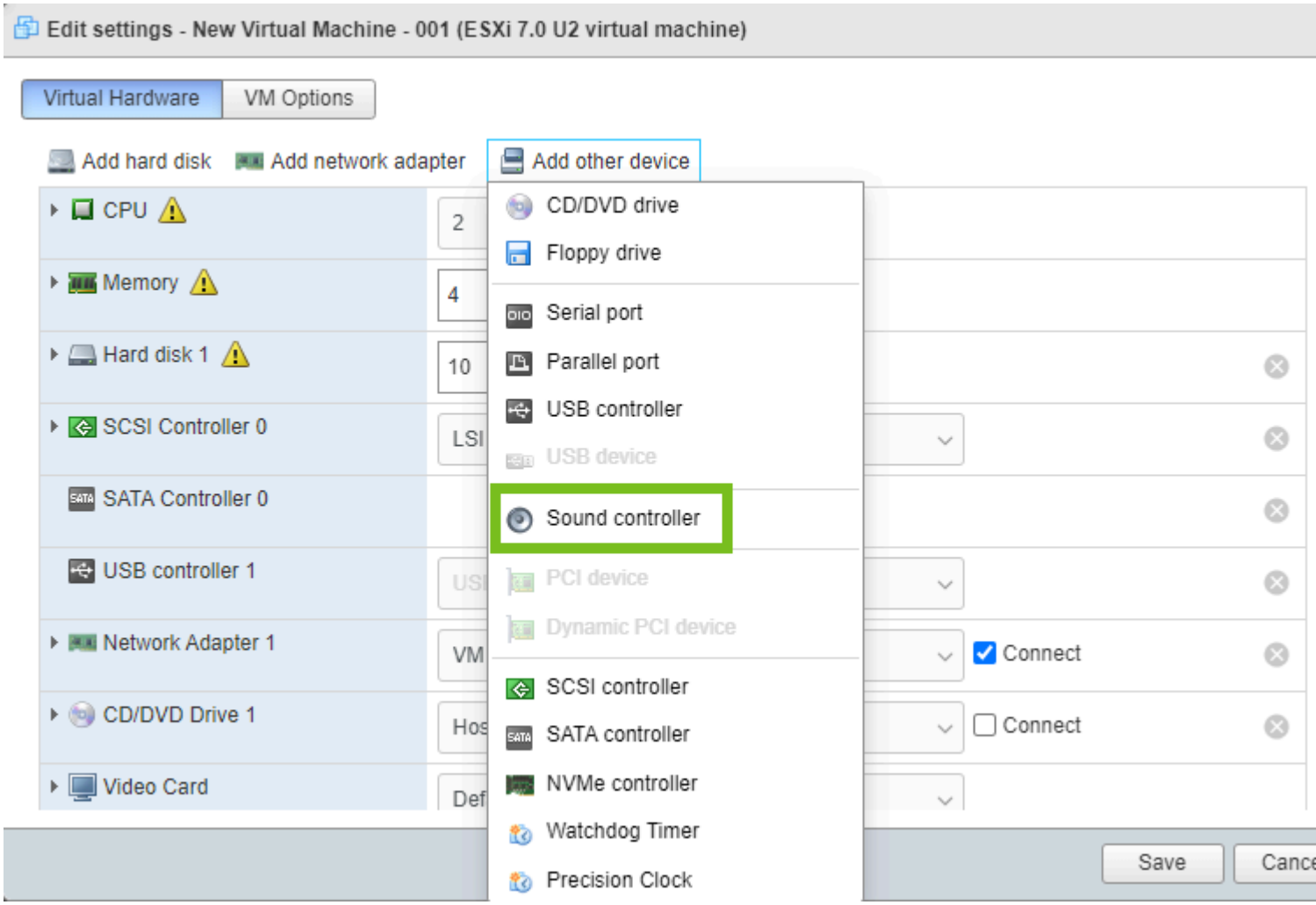
1. Click **Virtual Machines** in the inventory.
2. Right-click the virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **USB device** from the drop-down menu.
   The USB device appears in the hardware list of available hardware devices for the virtual machine.

4. From the **USB device** drop-down, select which USB device to add to the virtual machine.
5. Click **Save**.

Add a Sound Controller to a Virtual Machine in the VMware Host Client

By using the VMware Host Client, you can add a sound controller to a virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **Sound controller** from the drop-down menu.



The sound controller appears in the list of available hardware devices for the virtual machine.

4. From the **Sound card** drop-down menu, select which sound controller to connect to the virtual machine.
5. Click **Save**.

Parallel and Serial Port Configuration in the VMware Host Client

Parallel and serial ports are interfaces for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port or to a file on the host computer. You can also use it to establish a direct connection between two

virtual machines or a connection between a virtual machine and an application on the host computer. You can add parallel and serial ports and change the serial port configuration.

Add a Serial Port to a Virtual Machine in theVMware Host Client

A virtual machine can use up to four virtual serial ports. You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side-named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or a Virtual Serial Port Concentrator (vSPC) URI to connect a serial port over the network.

- Familiarize yourself with the different media types that the port can access, vSPC connections, and any conditions that might apply. See *vSphere Virtual Machine Administration*.
- To connect a serial port over a network, add a Firewall rule set. See *vSphere Virtual Machine Administration*.
- Required privilege:**Virtual Machine** > **Configuration** > **Add or Remove Device**

  Power off the virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **Serial Port**.

   The Serial Port appears in the hardware list.
4. In the hardware list, expand the serial port and select the type of media port to access.

Option	Description
Use output file	Browse to the location of the file on the host to store the output of the virtual serial port.
Use physical serial port	Select the port from the drop-down menu.
Use named pipe	1. Type a name for the pipe in the **Pipe name** field 2. Select the **Near End** and **Far End** of the pipe from the drop-down menus.
Use network	1. From the **Direction** drop-down menu, select **Server** or **Client**. 2. Type the port URI. The URI is the remote end of the serial port to which the serial port of the virtual machine should connect. 3. If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select **Use Virtual Serial Port Concentrator** and enter the vSPC URI location.

5. Optional: Deselect **Connect at power on** if you do not want the parallel port device to connect when the virtual machine powers on.
6. Click **Save**.

Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Add a Parallel Port to a Virtual Machine in the VMware Host Client
To connect peripheral devices to virtual machines, such as printers and scanners, you can use a parallel port. You send the output of such devices to a file on the host computer.

- Power off the virtual machine.
- Verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.

Note: To add a parallel port to a virtual machine that runs on an ESXi 4.1 or earlier host, you can also select to send output to a physical parallel port on the host. This option is not available with ESXi 5.0 and later host versions.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **Parallel Port**.
   The parallel port appears in the hardware list.
4. Expand the parallel port and in the Connection field, browse to a folder to create the file in.
   The file path appears in the **Connection** text box.
5. Optional: Select **Connect at power on** to configure the device to connect when the virtual machine powers on.
6. Click **Save**.

Using a Virtual Watchdog Timer

To ensure self-reliance related to the system performance within a virtual machine, you can add a virtual Watchdog Timer (VWDT) device. If the guest operating system stops responding and cannot recover on its own due to software glitches or errors, the VWDT waits for a predefined period of time and then restarts the system.

You can enable the VWDT to start either by the guest operating system, or by the BIOS or EFI firmware. If you chose the VWDT to start by the BIOS or EFI firmware, it starts before the guest operating system boots.

The VWDT has an important role in guest-based clustering solutions where each virtual machine in the cluster can recover on its own if it fails.

Add a Virtual Watchdog Timer Device to a Virtual Machine in the VMware Host Client
You can add a virtual Watchdog Timer device to a virtual machine to prevent the virtual machine from a guest operating system failure for an extended period of time.

- Power off the virtual machine.
- Verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.
- Verify that the guest operating system of the virtual machine supports the VWDT device.
- Verify that the virtual hardware version is 17.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and click **Watchdog Timer**.
   The Watchdog Timer device appears in the hardware list.
4. Optional: Select **Start with BIOS/EFI boot** to start the watchdog timer by the BIOS or EFI firmware.
   When you select this option, the VWDT device starts before the guest operating system. If the Guest OS boot takes too long or does not support the watchdog timer, the device might constantly restart the virtual machine.

5. Click **Save**.

Add a Precision Clock Device to a Virtual Machine in the VMware Host Client

A precision clock is a virtual device that runs on a virtual machine and accesses the system time of a host. By adding a precision clock to a virtual machine, you ensure time synchronization and high precision timestamping.

- Power off the virtual machine.
- Verify that the virtual hardware version is 17.
- Verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.
- Verify that you have the **Virtual machine** > **Configuration** > **Modify device settings** privilege on the virtual machine.

1. In the VMware Host Client inventory, click **Virtual Machines**.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, click **Add other device** and select **Precision Clock**.
   The precision clock device appears in the hardware list.
4. Optional: Select the time synchronization protocol.
5. Click **Save**.

Add a PCI Device to a Virtual Machine in the VMware Host Client

DirectPath I/O allows the guest operating system of a virtual machine to access the physical PCI and PCIe devices connected to a host directly. By using this technology, you can connect each virtual machine to up to sixteen physical PCI devices. You can use Dynamic DirectPath I/O to assign multiple PCI passthrough devices to a virtual machine. Starting with vSphere 7.0, you can identify the PCI passthrough devices by their vendor and model name.

- Power off the virtual machine.
- Verify that you have the **Virtual machine** > **Configuration** > **Add or remove device** privilege on the virtual machine.
- Verify that the PCI devices are connected to the host and marked as available for passthrough.
- If you want to add a dynamic PCI device to a virtual machine, verify that the virtual hardware version is 17.

Note: Some virtual machine operations become unavailable when you add a PCI or PCIe passthrough device to the virtual machine.

For information about the hardware label configuration, see Change the Hardware Label in the VMware Host Client.

1. In the VMware Host Client inventory, click **Virtual Machines**.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, click **Add other device** and select a device.

Option	Action
PCI device	1. Click **PCI device**. A new device appears in the hardware list. 2. From the drop-down menu, select a PCI device to connect to the virtual machine.
Dynamic PCI device	1. Click **Dynamic PCI device**. A new device appears in the hardware list.

Option	Action
	2. Expand **New PCI device**, and from the drop-down menu, select the PCI passthrough devices to connect to the virtual machine. You can identify PCI passthrough devices by vendor, model name, and hardware label. Hardware labels, if present, are displayed in brackets. **Note:** When you add a PCI device to a virtual machine, the full memory size of the virtual machine is automatically reserved.

4. Click **Save**.

Securing Virtual Machines with Intel Software Guard Extensions

By using the , you can configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines and provide additional security to your workloads.

Some modern Intel CPUs implement a security extension called Intel® Software Guard Extensions (Intel SGX). Intel SGX is a processor-specific technology that defines private regions of memory, called enclaves. Intel SGX protects the enclave contents from disclosure and modification in such a way that code running outside the enclave cannot access them.

vSGX enables virtual machines to use Intel SGX technology if available on the hardware. To use vSGX, the ESXi host must be installed on an SGX-capable CPU and SGX must be enabled in the BIOS of the ESXi host. You can use the vSphere Client to enable SGX for a virtual machine.

Enable vSGX on a Virtual Machine in theVMware Host Client

To protect the enclave contents from disclosure and modifications, you can enable vSGX on a virtual machine in theVMware Host Client.

- Power off the virtual machine.
- Verify that the virtual machine uses EFI firmware.
- Verify that theESXi host is version 7.0 or later.
- Verify that the guest operating system in the virtual machine is Linux, Windows 10 (64-bit) or later, or Windows Server 2016 (64-bit) or later.
- Verify that you have the**Virtual machine** > **Configuration** > **Modify device settings** privilege on the virtual machine.
- Verify that theESXi host is installed on an SGX-capable CPU, and SGX is enabled in the BIOS of theESXi host. For information about the supported CPUs, see https://kb.vmware.com/s/article/71367.

Some operations and features are not compatible with SGX.

- Migration with Storage vMotion
- Suspending or resuming the virtual machine
- Taking a snapshot of the virtual machine
- Fault Tolerance

- Enabling Guest Integrity (GI, platform foundation for VMware AppDefense 1.0)

1. In theVMware Host Client inventory, click **Virtual Machines**.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, expand **Security devices**.
4. Select the **Enable** check box.
5. Under **Enclave page cache size**, enter a new value in the text box and select the size in MB or GB from the drop-down menu.

   Note: The enclave page cache size must be a multiple of 2.
6. From the **Launch control configuration** drop-down menu, select the appropriate mode.

Option	Action
Locked	Enables the launch enclave configuration. Under **Launch enclave public key hash**, enter a valid SHA256 hash. The SHA256 hash key must contain 64 characters.
Unlocked	Enables the launch enclave configuration of the guest operating system.

7. Click **Save**.

Disable vSGX on a Virtual Machine in the VMware Host Client

To disable vSGX on a virtual machine, you can use the VMware Host Client.

1. In the VMware Host Client inventory, click **Virtual Machines**.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, expand **Security devices**.
4. Deselect the **Enable** check box and click **Save**.

vSGX is disabled on the virtual machine.

Managing Virtual Machines in the VMware Host Client

After creating a virtual machine in the VMware Host Client, you can perform different management tasks on the virtual machine, including deleting the virtual machine from the host, remove the virtual machine from a datastore, registering it back on a datastore, and so on. You can also return the virtual machine to the host.

Access a Virtual Machine in the VMware Host Client

You can access the virtual machines on the host that you are logged in to, to configure the virtual machine hardware and options, to perform administrative tasks, and to perform basic troubleshooting tasks.

To display a virtual machine in the VMware Host Client inventory, power on the virtual machine.

To access the virtual machines that are available on the host that you are logged in to, click **Virtual Machines** in the VMware Host Client inventory.

The list of available virtual machines is displayed under **Virtual Machines**.

You can now edit the virtual machine settings and perform different administrative and troubleshooting tasks on the virtual machines in the list.

Power States of a Virtual Machine in the VMware Host Client

The basic power operations for a virtual machine include powering on, powering off, suspending, and reset.

- Verify that you have the **VirtualMachine** > **Interaction** > **PowerOn** privilege.
- Verify that you have the **VirtualMachine** > **Interaction** > **PowerOff** privilege.
- Verify that you have the **VirtualMachine** > **Interaction** > **Suspend** privilege.
- Verify that you have the **VirtualMachine** > **Interaction** > **Reset** privilege.

For information about how to change the virtual machine power states, see Configure the Virtual Machine Power States in theVMware Host Client.

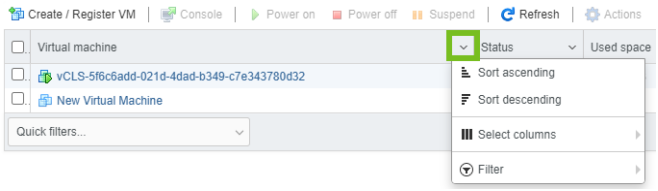
1. In the VMware Host Client inventory, click **Virtual Machines**.
2. Right-click a virtual machine and select a power operation.

Option	Description
Power On ( )	Powers on a virtual machine when the virtual machine is stopped.
Power off ( )	Powers off a virtual machine and shuts down the guest operating system. Powering off a virtual machine might cause loss of data.
Suspend ( )	Suspends a running virtual machine and leaves it connected to the network. When you resume a suspended virtual machine, the virtual machine continues operating at the same point the virtual machine was at when it was suspended.
Reset ( )	Shuts down and restarts the guest operating system without powering off the virtual machine.

Use Virtual Machine Column Configuration in the VMware Host Client

The virtual machines panel in the VMware Host Client allows you to configure the information that you want to display. You can show or hide different columns, such as status, used space, host name, host CPU, and so on.

1. Click **Virtual Machines** in the inventory.
2. In the list of virtual machines, click the down arrow icon next to any column title and select **Select**



columns.

The list with all available columns appears.

3. Select the information that you want to display in the virtual machine panel.

Remove Virtual Machines from a Host in the VMware Host Client

You can unregister a virtual machine if you want to keep it on the datastore, but you no longer want the VMware Host Client inventory to display the virtual machine.

Power off the virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click the virtual machine from the list and select **Unregister**.
3. To confirm that you want to remove the virtual machine from the inventory, click **Yes**.

The host removes the virtual machine from the inventory and no longer tracks its condition.

Remove Virtual Machines from a Datastore in the VMware Host Client

To free space on the datastore, you can remove the virtual machines that you no longer need. Removing a virtual machine from the VMware Host Client inventory deletes all virtual machine files from the datastore, including the configuration file and virtual disk files. You can delete multiple virtual machines

- Power off the virtual machine.
- Verify that the virtual machine does not share the disk with another virtual machine. If two virtual machines share one disk, the disk files are not deleted.

1. Click **Virtual Machines** in the inventory.
2. Select one or multiple check boxes next to the virtual machines that you want to remove and select **Actions** > **Delete**.
   The **Delete VMs** dialog box opens.
3. Click **Delete**.

Register a Virtual Machine in the VMware Host Client

If you remove a virtual machine or template from a host but do not remove it from the host datastore, you can return it to the host's inventory.

1. Click **Storage** in the VMware Host Client inventory.
2. Right-click a datastore from the list and click **Register a VM**.
3. Select the virtual machine you want to register from the list and click **Register**.

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. When you take a snapshot of a virtual machine, an image of the virtual machine in a given state is copied and stored. Snapshots are useful when you want to revert repeatedly to a virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking a snapshot of a VM for each member of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before you change a virtual machine.

Several operations for creating and managing virtual machine snapshots and snapshot trees are available in the vSphere Client. These operations enable you to create snapshots, revert any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create snapshot trees where you save the virtual machine state at any specific time so that you can revert that virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes the disks added or changed after you take the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.

The Snapshot Hierarchy

The vSphere Client presents the snapshot hierarchy as a tree with one or more branches. Snapshots in the hierarchy have parent to child relationships. In linear processes, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshot. Each parent snapshot can have more than one child. You can revert to the current parent snapshot or to any parent or child snapshot in the snapshot tree and create more snapshots from that snapshot. Each time you revert a snapshot and take another snapshot, a branch (child snapshot) is created.

Parent Snapshots	The first virtual machine snapshot that you create is the base parent snapshot. The parent snapshot is the most recently saved version of the current state of the virtual machine. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base `.vmdk` file. The parent snapshot is always the snapshot that appears immediately above the **You are here** icon in the Snapshot Manager. If you revert a snapshot, that snapshot becomes the parent of the **You are here** current state. **Note:** The parent snapshot is not always the snapshot that you took most recently.
Child Snapshots	A snapshot of a virtual machine taken after the parent snapshot. Each child snapshot contains delta files for each attached virtual disk, and optionally a memory file that points from the present state of the virtual disk (You are here). Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.

The relationship of parent and child snapshots can change if you have multiple branches in the snapshot tree. A parent snapshot can have more than one child. Many snapshots have no children.

CAUTION: Do not manually manipulate individual child disks or any of the snapshot configuration files because doing so can compromise the snapshot tree and result in data loss. This restriction includes disk resizing and making modifications to the base parent disk by using the `vmkfstools` command.

Snapshot Behavior

Taking a snapshot preserves the disk state at a specific time by creating a series of delta disks for each attached virtual disk or virtual RDM and optionally preserves the memory and power state by creating a memory file. Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings.

Each snapshot creates an additional delta `.vmdk` disk file. When you take a snapshot, the snapshot mechanism prevents the guest operating system from writing to the base `.vmdk` file and instead directs all writes to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the previous snapshot. If more than one snapshot exists, delta disks can represent the difference between each snapshot. Delta disk files can expand quickly and become as large as the entire virtual disk if the guest operating system writes to every block of the virtual disk.

Snapshot Files

When you take a snapshot, you capture the state of the virtual machine settings and the virtual disk. If you are taking a memory snapshot, you also capture the memory state of the virtual machine. These states are saved to files that reside with the virtual machine's base files.

Snapshot Files

A snapshot consists of files that are stored on a supported storage device. A Take Snapshot operation creates `.vmdk`, `-delta.vmdk`, `.vmsd`, and `.vmsn` files. By default, the first and all delta disks are stored with the base `.vmdk` file. The `.vmsd` and `.vmsn` files are stored in the virtual machine directory.

Delta disk files	A `.vmdk` file to which the guest operating system can write. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that the previous snapshot was taken. When you take a snapshot, the state of the virtual disk is preserved, the guest operating system stops writing to it, and a delta or child disk is created. A delta disk has two files. One is a small descriptor file that contains information about the virtual disk, such as geometry and child-parent relationship information. The other one is a corresponding file that contains the raw data. The files that make up the delta disk are called child disks or redo logs.
Flat file	A `-flat.vmdk` file that is one of two files that comprises the base disk. The flat disk contains the raw data for the base disk. This file does not appear as a separate file in the Datastore Browser.
Database file	A `.vmsd` file that contains the virtual machine's snapshot information and is the primary source of information for the Snapshot Manager. This file contains line entries, which define the relationships between snapshots and between child disks for each snapshot.
Memory file	A `.vmsn` file that includes the active state of the virtual machine. Capturing the memory state of the virtual machine lets you revert to a turned on virtual machine state. With nonmemory snapshots, you can only revert to a turned off virtual machine state. Memory snapshots take longer to create than nonmemory snapshots. The time the ESXi host takes to write the memory onto the disk depends on the amount of memory the virtual machine is configured to use.

A **Take Snapshot** operation creates `.vmdk`, `-delta.vmdk`, `vmsd` or `-sesparse.vmdk`, and `vmsn` files.

SEsparse is a default format for all delta disks on the VMFS6 datastores.

File	Description
vmname-number`.vmdk`, *vmname-number*`-delta.vmdk`, *vmname-number*`-sesparse.vmdk`	Snapshot file that represents the difference between the current state of the virtual disk and the state that existed at the time the previous snapshot was taken.

File	Description
	The filename uses the following syntax, `S1vm-000001.vmdk` where `S1vm` is the name of the virtual machine and the six-digit number, `000001`, is based on the files that already exist in the directory. The number does not consider the number of disks that are attached to the virtual machine.
vmname`.vmsd`	Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.
vmname`-.Snapshot`*number*`.vmsn`	Memory state of the virtual machine at the time you take the snapshot. The filename uses the following syntax, `S1vm.snapshot1.vmsn` , where `S1vm` is the virtual machine name, and `snapshot1` is the first snapshot. **Note:** A `.vmsn` file is created each time you take a snapshot, regardless of the memory selection. A `.vmsn` file without memory is much smaller than one with memory.

Snapshot Limitations

Snapshots can affect the virtual machine performance and do not support some disk types or virtual machines configured with bus sharing. Snapshots are useful as short-term solutions for capturing point-in-time virtual machine states and are not appropriate for long-term virtual machine backups.

- VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.
- Virtual machines with independent disks must be powered off before you take a snapshot.
- Starting with ESXi 7.0 Update 3l, you can take a memory snapshot of a virtual machine with an independent disk only to analyze the guest operating system behavior of a virtual machine. You cannot use such snapshots for virtual machine backups because restoring this type of snapshots is unsupported.
- Quiesced snapshots require VMware Tools installation and guest operating system support.
- Snapshots are not supported with PCI vSphere DirectPath I/O devices.
- VMware does not support snapshots of virtual machines configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine currently has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.
- Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost. Also, large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected if there is hardware failure.
- Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot. Also, you might see a delay in the amount of time it takes the virtual machine to power on. Do not run production virtual machines from snapshots on a permanent basis.

Taking Snapshots of a Virtual Machine

You can take one or more snapshots of a virtual machine to capture the settings state, disk state, and memory state at different specific times. When you take a snapshot, you can also quiesce the virtual machine files and exclude the virtual machine disks from snapshots.

When you take a snapshot, other activity that is occurring in the virtual machine might affect the snapshot process when you revert to that snapshot. The best time to take a snapshot from a storage perspective, is when you are not incurring a

large I/O load. The best time to take a snapshot from a service perspective is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails. Depending on the task that you are performing, you can create a memory snapshot or you can quiesce the file system in the virtual machine.

Memory Snapshots	The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state. When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.
Quiesced Snapshots	When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files. If the virtual machine is powered off or VMware Tools is not available, the `Quiesce` parameter is not available. You cannot quiesce virtual machines that have large capacity disks.

Important: Do not use snapshots as your only backup solution or as a long-term backup solution.

Take a Snapshot in the VMware Host Client

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. To take a snapshot of a suspended virtual machine, wait until the suspend operation finishes before you take a snapshot.

- If you are taking a memory snapshot of a virtual machine that has multiple disks in different disk modes, verify that the virtual machine is powered off. For example, if you have a special purpose configuration that requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.
- To capture the memory state of the virtual machine, verify that the virtual machine is powered on.
- To quiesce the virtual machine files, verify that the virtual machine is powered on and that VMware Tools is installed.
- Verify that you have the **Virtual machine** > **Snapshot management** > **Create snapshot** privilege on the virtual machine.

When you create a memory snapshot, the snapshot captures the state of the virtual machine's memory and the virtual machine power settings. Snapshots that capture the memory state of a virtual machine take longer to complete. You might also see a momentary lapse in response over the network.

When you quiesce a virtual machine, VMware Tools quiesces the file system in the virtual machine. The quiesce operation pauses or alters the state of running processes on the virtual machine, especially processes that might modify information stores on the disk during a restore operation.

Application-consistent quiescing is not supported for virtual machines with IDE or SATA disks.

Note: If you take a snapshot of a Dynamic Disk (Microsoft-specific disk type), the snapshot technology preserves the quiesced state of the file system, but does not preserve the quiesced state of the application.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine from the list and select **Snapshots** > **Take snapshot**.
3. Enter a name for the snapshot.
4. Optional: Type a description for the snapshot.
5. Optional: Select the **Snapshot the virtual machine's memory** check box to capture the memory of the virtual machine.
6. Optional: Deselect **Snapshot the virtual machine's memory** and select **Quiesce guest file system (needs VMware Tools installed)** check box to pause running processes on the guest operating system so that file system contents are in a known consistent state when you take the snapshot.

   Quiesce the virtual machine files only when the virtual machine is powered on and you do not want to capture the virtual machine's memory.
7. Click **Take snapshot**.

Restoring Snapshots

To return a virtual machine to its original state, or to return to another snapshot in the snapshot hierarchy, you can restore a snapshot.

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot. If you want the virtual machine to be suspended, powered on, or powered off when you start it, make sure that it is in the correct state when you take the snapshot.

You can restore snapshots in the following ways:

Revert to Latest Snapshot	Restores the parent snapshot, one level up in the hierarchy from the **You are Here** position. **Revert to Latest Snapshot** activates the parent snapshot of the current state of the virtual machine.
Revert To	Lets you restore any snapshot in the snapshot tree and makes that snapshot the parent snapshot of the current state of the virtual machine. Subsequent snapshots from this point create a new branch of the snapshot tree.

Restoring snapshots has the following effects:

- The current disk and memory states are discarded, and the virtual machine reverts to the disk and memory states of the parent snapshot.
- Existing snapshots are not removed. You can restore those snapshots at any time.
- If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot.

Table 527: Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Note: vApp metadata for virtual machines in vApps does not follow the snapshot semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

Revert to the Latest Snapshot in the VMware Host Client

Revert to a snapshot to restore the virtual machine to the state of the snapshot.

Verify that you have the **Virtual machine** > **Snapshot management** > **Revert to snapshot** privilege on the virtual machine.

1. Click **Virtual Machines** in the inventory.
2. Right-click the virtual machine in the list and select **Snapshots** > **Restore snapshot**.

   Note: The current state of the virtual machine will be lost unless you save it in a snapshot.
3. Click **Restore** to revert the virtual machine to the most recent snapshot.

Deleting Snapshots

Deleting a snapshot removes the snapshot from the Snapshot Manager. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk.

Deleting a snapshot does not change the virtual machine or other snapshots. Deleting a snapshot consolidates the changes between snapshots and previous disk states and writes all the data from the delta disk that contains the information about the deleted snapshot to the parent disk. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

To delete a snapshot, a large amount of information needs to be read and written to a disk. This process can reduce virtual machine performance until consolidation is complete. Consolidating snapshots removes redundant disks, which improves virtual machine performance and saves storage space. The time it takes to delete snapshots and consolidate the snapshot files depends on the amount of data that the guest operating system writes to the virtual disks after you take the last snapshot. The required time is proportional to the amount of data the virtual machine is writing during consolidation if the virtual machine is powered on.

Failure of disk consolidation can reduce the performance of virtual machines. You can check whether any virtual machines require separate consolidation operations by viewing a list. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see *vSphere Virtual Machine Administration*.

Delete

Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. **Delete** writes disk changes that occur between the state of the snapshot and the previous disk state to the parent snapshot.

Note: Deleting a single snapshot preserves the current state of the virtual machine and does not affect any other snapshot.

	You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.
Delete All	Use the **Delete All** option to delete all snapshots from the Snapshot Manager. **Delete all** consolidates and writes the changes that occur between snapshots and the previous delta disk states to the base parent disk and merges them with the base virtual machine disk.

To prevent snapshot files from merging with the parent snapshot if, for example, an update or installation fails, first use the **Restore** command to restore to a previous snapshot. This action invalidates the snapshot delta disks and deletes the memory file. You can then use the **Delete** option to remove the snapshot and any associated files.

Delete a Snapshot in the VMware Host Client

You can use the Snapshot Manager to delete a single snapshot or all snapshots in a tree.

Be careful not to accidentally delete a snapshot that you need. You cannot restore a deleted snapshot. For example, you might want to install several browsers, a, b, and c, and capture the virtual machine state after you install each browser. The first, or base snapshot, captures the virtual machine with browser a and the second snapshot captures browser b. If you restore the base snapshot that includes browser a and take a third snapshot to capture browser c and delete the snapshot that contains browser b, you cannot return to the virtual machine state that includes browser b.

1. Click **Virtual Machines** in the inventory.
2. Right-click the virtual machine in the list and select **Snapshots** > **Manage Snapshots**.
3. Click the snapshot that you want to delete and click **Delete snapshot**.
4. Optional: In the **Delete Snapshot** dialog box, select the **Remove all children snapshots** check-box to delete the selected snapshot together with all its children snapshots.
5. Click **Remove** to confirm the deletion.
6. Click **Close** to navigate out of the Snapshot Manager.

Managing Snapshots with the VMware Host Client

You can review all snapshots for your virtual machines and use the Snapshot Manager to manage the snapshots.

After you take a snapshot, you can right-click a virtual machine and click **Revert to snapshot** to restore the virtual machine to the state of the snapshot at any time.

If you have a series of snapshots, you can use the Snapshot Manager to restore any parent or child snapshot. Subsequent child snapshots that you take from the restored snapshot create a branch in the snapshot tree. Use the Snapshot Manager to delete a snapshot from the tree.

Table 528: Snapshot Manager

Option	Description
Snapshot tree	Displays all snapshots for the virtual machine.
You are here icon	The **You are here** icon represents the current and active state of the virtual machine. The **Restore**, **Delete**, and **Edit** actions are disabled for the **You are here** state.
Take, **Restore**, **Delete**, **Edit**	Snapshot options.
Details	Shows the snapshot name and description, the date you created the snapshot. The Console shows the power state of the virtual machine when a snapshot was taken. The Name, Description, and Created text boxes are blank if you do not select a snapshot.

Monitoring a Virtual Machine in the VMware Host Client

You can monitor various performance aspects and keep track of the actions that take place on virtual machines that you create in the VMware Host Client.

View Virtual Machine Performance Charts in the VMware Host Client

You can view line charts with information about the resource usage of virtual machines that you create in the VMware Host Client.

1. Click **Virtual Machines** in the inventory.
2. Click a virtual machine from the list.
3. Expand the virtual machine in the inventory and click **Monitor**.
4. Click **Performance**.
5. To view the virtual machine resource usage for the last hour, select an option from the drop-down menu.
   - To view the percentage of CPU that the virtual machine used during the last hour, select **CPU usage**.
   - To view the memory that the host consumed during the last hour, select **Memory usage**.

View Virtual Machine Events in the VMware Host Client

Events are records of the actions that a user performs on a virtual machine. When you create a virtual machine in the VMware Host Client, you can view the events associated with the virtual machine.

Required privilege: **Read only**.

1. Click **Virtual Machines** in the inventory.
2. Click a virtual machine from the list.
3. Expand the virtual machine in the inventory and click **Monitor**.
4. Click **Events**.
   A list of all virtual machine events is displayed.

5. Optional: Click an event from the list to view event details.
6. Optional: Use the filter controls above the list to filter the list.
7. Optional: Click a column heading to sort the list.

View Virtual Machine Tasks in the VMware Host Client

When you create a virtual machine in the VMware Host Client, you can view all virtual machine tasks and information about the task target, initiator, queue time, start time, result, and time of completion.

1. Click **Virtual Machines** in the inventory.
2. Click a virtual machine from the list.
3. Expand the virtual machine in the inventory and click **Monitor**.
4. Click **Tasks**.
5. Optional: Click on a task from the list to view task details.
6. Optional: Use the filter controls above the list to filter the list.
7. Optional: Click a column heading to sort the list.

View Virtual Machine Log Browser in the VMware Host Client

Generate and monitor logs for the host that you are managing by using the VMware Host Client. Use the logs to diagnose and troubleshoot various issues with your host environment.

1. Click **Virtual Machines** in the inventory.
2. Click a virtual machine from the list.
3. Expand the virtual machine in the inventory and click **Monitor**.
4. Click **Logs**.
5. Optional: Click **Generate support bundle** to consolidate all the logs for troubleshooting.
6. Right-click a log from the list and select **Open in new window** to view the log.

View Virtual Machine Notifications in the VMware Host Client

You can view virtual machine notifications and information about related tasks, which you can perform, for virtual machines that you create in the VMware Host Client.

1. Click **Virtual Machines** in the inventory.
2. Click a virtual machine from the list.
3. Expand the virtual machine in the inventory and click **Monitor**.
4. Click **Notifications**.
   A list with all virtual machine notifications is displayed.
5. Optional: Click a notification to view details.
6. Optional: Click a notification and click **Actions** to view suggested tasks.

Securing Virtual Machines in the VMware Host Client

The guest operating system that runs in the virtual machine is vulnerable to the same security risks as any physical system. To boost security in your virtual environment, you can add a virtual Trusted Platform Module (vTPM) to your ESXi

hosts. You can also enable virtualization-based security (VBS) for the virtual machines that run the latest Windows 10 and Windows Server 2016 operating systems.

Using Virtual TPM in the VMware Host Client

The Trusted Platform Module (TPM) is a specialized chip that stores host-specific sensitive information, for example private keys and OS secrets. The TPM chip is also used to perform cryptographic tasks and attest the integrity of the platform.

The virtual TPM device is a software emulation of the TPM functionality. You can add a virtual TPM (vTPM) device to the virtual machines in your environment. The vTPM implementation does not require a physical TPM chip on the host. ESXi uses the vTPM device to exert the TPM functionality in your vSphere environment.

vTPM is available to virtual machines that have Windows 10 and Windows Server 2016 operating systems. The virtual machine must be of hardware version 14 or later.

You can add a virtual TPM device to a virtual machine only in the vCenter Server instance. For more information, see the *vSphere Security* documentation.

In the VMware Host Client, you can only remove the virtual TPM device from a virtual machine.

Using VBS in the VMware Host Client

Virtualization-based security (VBS) uses the Microsoft Hyper-V based virtualization technology to isolate core Windows OS services in a separate virtualized environment. Such isolation provides an additional level of protection, because it makes it impossible for the key services in your environment to be manipulated.

Enabling VBS on a virtual machine automatically enables the virtual hardware that Windows requires for the VBS feature. By enabling VBS, a variant of Hyper-V starts in the virtual machine and Windows starts running inside the Hyper-V root partition.

VBS is available on the latest Windows OS versions, for example Windows 10 and Windows Server 2016. To use VBS on a virtual machine, the virtual machine compatibility must be ESXi 6.7 and later.

In the VMware Host Client, you can enable VBS during a virtual machine creation. Alternatively, you can enable or disable VBS for an existing virtual machine.

Note: You can enable VBS on a virtual machine only if the TPM validation of the host is successful.

Remove a vTPM device from a VM in the VMware Host Client

In the VMware Host Client, you can only remove the vTPM device from a virtual machine.

- The virtual machine must be of hardware version 14 or later.
- The guest OS must be Windows 10 or Windows Server 2016 and later.
- The virtual machine must be powered off.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, find the TPM device and click the **Remove** icon.
   The virtual TPM device is removed from the virtual machine.

4. Click **Save** to close the wizard.

Enable or Disable Virtualization-based Security on an Existing VM in the VMware Host Client

You can enable Microsoft virtualization-based security (VBS) on existing virtual machines for supported Windows guest operating systems.

Enabling VBS is a process that involves first enabling VBS in the virtual machine then enabling VBS in the guest operating system.

Note: New virtual machines configured for Windows 10, Windows Server 2016, and Windows Server 2019 on hardware versions less than version 14 are created using Legacy BIOS by default. If you change the firmware type of a virtual machine from Legacy BIOS to UEFI, you must reinstall the guest operating system.

See the *vSphere Security* documentation for information about acceptable CPUs and VBS best practices.

Using Intel CPUs for VBS requires vSphere 6.7 or later. The virtual machine must have been created using hardware version 14 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit) or later releases
- Windows Server 2016 (64 bit) or later releases

Using AMD CPUs for VBS requires vSphere 7.0 Update 2 or later. The virtual machine must have been created using hardware version 19 or later and one of the following supported guest operating systems:

- Windows 10 (64 bit), version 1809 or later releases
- Windows Server 2019 (64 bit) or later releases

Ensure that you install the latest patches for Windows 10, version 1809, and Windows Server 2019, before enabling VBS.

For more information about enabling VBS on virtual machines on AMD platforms, see the VMware KB article at https://kb.vmware.com/s/article/89880.

1. Click **Virtual Machines** in the inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **VM Options** tab, enable or disable VBS for the virtual machine.
   - To enable VBS for the virtual machine, select the **Enable Virtualization Based Security** check box.
   - To disable VBS for the virtual machine, deselect the **Enable Virtualization Based Security** check box.

   When you enable VBS, several options are automatically selected and become dimmed in the wizard.
4. Click **Save** to close the wizard.

Managing Storage in the VMware Host Client

When you connect to an ESXi host by using the VMware Host Client, you can perform different storage management tasks on the ESXi host, including configuring adapters, creating datastores, and viewing storage device information.

Working with Datastores in the VMware Host Client

Datastores are logical containers, similar to file systems, that contain specific information of each storage device and provide a uniform model for storing virtual machine files. You can also use datastores to store ISO images, virtual machine templates, and floppy images.

Depending on the type of storage you use, datastores can be of the following types:

- Virtual Machine File System (VMFS)
- Network File System (NFS)

You can increase datastore capacity after you create a datastore but only if it is a VMFS datastore.

View Datastore Information in the VMware Host Client

Use the VMware Host Client to display the datastores available to the hosts and analyze their properties.

1. Click **Storage** in the VMware Host Client inventory and click **Datastores**.
2. To view the details for a specific datastore, select the datastore from the list.

Create a VMFS Datastore in theVMware Host Client

VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that your host detects, including Fibre Channel, iSCSI, and local storage devices.

Install and configure any adapters that your storage requires. Rescan the adapters to discover newly added storage devices.

To create datastores in theVMware Host Client, you can use the **New datastore** wizard.

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **New datastore.**

   The **New datastore** wizard opens.
3. On the Select creation type page, select **Create new VMFS datastore** and click **Next**.

Option	Description
Create new VMFS datastore	Creates a new VMFS datastore on a local disk device.
Add an extent to existing VMFS datastore	Increases the size of an existing datastore by adding a new extent on another disk.
Expand an existing VMFS datastore extent	Increases the size of an existing datastore extent.
Mount NFS datastore	Creates a new datastore by mounting a remote NFS volume.

4. On the Select device page, select where to create the new VMFS partition.
   a) Enter a name for the new datastore.
   b) Select a device to add the datastore to.

      The list contains only devices that have enough available space.
   c) Click **Next**.
5. On the Select partitioning options page, select how to partition the device and click **Next**.

Option	Description
Use Full Disk	It shows you all the free space that is available on the device.
Custom	Click the **Free space** bar and use the horizontal scroller to partition the device.

6. On the Ready to complete page, review the configuration details and click **Finish**.

Increasing VMFS Datastore Capacity

If your VMFS datastore requires more space, increase the datastore capacity. You can dynamically increase the capacity by growing a datastore extent or by adding an extent.

Use one of the following methods to increase the datastore capacity:

- Dynamically grow any expandable datastore extent, so that it fills the available adjacent capacity. The extent is considered expandable when the underlying storage device has free space immediately after the extent.
- Dynamically add the extent. The datastore can span over up to 32 extents with the size of each extent of more than 2 TB, yet appear as a single volume. The spanned VMFS datastore can use any or all its extents at any time. It does not need to fill up a particular extent before using the next one.

Increase an Existing VMFS Datastore in theVMware Host Client

When you need to add virtual machines to a datastore, or when the virtual machines running on a datastore require more space, you can dynamically increase the capacity of a VMFS datastore.

If a shared datastore has powered on virtual machines and becomes 100% full, you can increase the datastore's capacity only from the host that the powered on virtual machines are registered on.

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **New datastore**.
3. On the Select creation type page, click **Add an extent to existing VMFS datastore** and click **Next**.
4. On the Select datastore page, select the datastore to expand and click **Next**.
5. On the Select device page, select a device to create the new VMFS partition on and click **Next**.
6. On the Select partitioning options page, select how to partition the device and click **Next**.

Option	Description
Use Full Disk	It shows you all the free space that is available on the device.
Custom	Click the **Free space** bar and use the horizontal scroller to partition the device.

7. On the Ready to complete page, review the configuration details and click **Finish**.

Mounting a Network File System Datastore in the VMware Host Client

With the VMware Host Client, you can create a Network File System (NFS) datastore to store virtual disks and to use as a central repository for ISO images, virtual machines, and so on. An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume that is located on a NAS server. vSphere supports versions 3 and 4.1 of the NFS protocol.

The ESXi host can mount an NFS volume and use it for its storage needs.

Typically, the NFS volume or directory is created by a storage administrator and is exported from the NFS server. You do not need to format the NFS volume with a local file system, such as VMFS. Instead, you mount the volume directly on the ESXi hosts and use it to store and boot virtual machines in the same way that you use the VMFS datastores.

In addition to storing virtual disks on NFS datastores, you can use NFS as a central repository for ISO images, virtual machine templates, and so on. If you use the datastore for the ISO images, you can connect the CD-ROM device of the virtual machine to an ISO file on the datastore. You then can install a guest operating system from the ISO file.

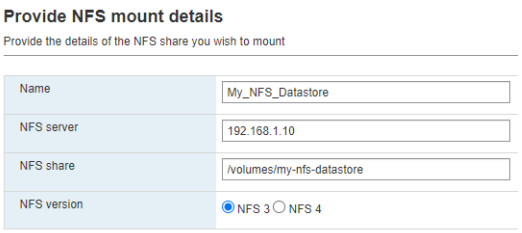
When you use NFS storage, follow the specific guidelines related to NFS server configuration, networking, NFS datastores, and so on.

Mount an NFS Datastore in the VMware Host Client

Use the **New datastore** wizard to mount a Network File System (NFS) datastore in the VMware Host Client.

Because NFS requires network connectivity to access data on remote servers, before configuring NFS, you must first configure VMkernel networking.

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **New datastore**.
   The **New datastore** wizard opens.
3. On the Select creation type page, click **Mount NFS datastore** and click **Next**.
4. On the Provide NFS mount details page, provide the details for the NFS you mount.



   a) Enter a name for the NFS datastore.
   b) Enter the NFS server name.
      For the server name, you can enter an IP address, a DNS name, or an NFS UUID.

      Note: When you mount the same NFS volume on different hosts, make sure that the server and folder names are identical across the hosts. If the names do not match, the hosts detect the same NFS volume as two different datastores. This might result in a failure of features such as vMotion. An example of such discrepancy is if you enter `filer` as the server name on one host and `filer.domain.com` on the other.
   c) Specify the NFS share.
   d) Specify the NFS version.
   e) Click **Next**.
5. On the Ready to complete page, review the configuration settings for the NFS datastore and click **Finish**.

Unmount a Datastore in the VMware Host Client

When you unmount a datastore in the VMware Host Client, it remains intact, but you can no longer view it in the inventory of the host that you manage. The datastore continues to appear on other hosts that it remains mounted on.

Note: Make sure that the datastore is not used by vSphere HA heartbeating. vSphere HA heartbeating does not prevent you from unmounting the datastore. However, if the datastore is used for heartbeating, unmounting it might cause the host to fail and restart all active virtual machines.

Before unmounting a datastore, also make sure that the following prerequisites are met:

- No virtual machines reside on the datastore.

- Storage DRS does not manage the datastore.
- Storage I/O Control is disabled for this datastore.

Do not perform any configuration operations that might result in I/O to the datastore while the unmounting is in progress.

1. Click **Storage** in the inventory and click **Datastores**.
2. Right-click the datastore to unmount from the list and click **Unmount**.
3. Confirm that you want to unmount the datastore.

Unmounting or Removing Datastore Fails

When you try to unmount or remove a datastore, the operation fails.

The operation to unmount or remove a datastore fails if the datastore has any opened files. For these user operations, the vSphere HA agent closes all the files that it has opened, for example, heartbeat files. If the agent is not reachable by vCenter Server or the agent cannot flush out pending I/Os to close the files, a `The HA agent on host '{hostName}' failed to quiesce file activity on datastore '{dsName}` fault is triggered.

If the datastore to be unmounted or removed is used for heartbeating, vCenter Server excludes it from heartbeating and chooses a new one. However, the agent does not receive the updated heartbeat datastores if it is not reachable, that is, if the host is isolated or in a network partition. In such cases, heartbeat files are not closed and the user operation fails. The operation can also fail if the datastore is not accessible because of storage failures such as all paths down.

Note: When you remove a VMFS datastore, the datastore is removed from all the hosts in inventory. So if there are any hosts in a vSphere HA cluster that are unreachable or that cannot access the datastore, the operation fails.

Ensure that the datastore is accessible and the affected hosts are reachable.

Using Datastore File Browser in the VMware Host Client

Use the datastore file browser to manage the contents of your datastore. You can perform a number of tasks that include uploading files to the datastore, downloading datastore files to your system, moving and copying datastore folders or files, and creating new datastore directories.

Upload Files to a Datastore in the VMware Host Client

Use the datastore file browser to upload files to datastores on your host.

Required privilege: **Datastore** > **Browse Datastore**

Note: Virtual Volumes do not support uploading files directly to the virtual datastores. You must first create a folder on the virtual datastore, and then upload the files into the folder.

In addition to their traditional use as a storage for virtual machine files, datastores can serve to store data or files related to virtual machines. For example, you can upload ISO images of operating systems from a local computer to a datastore on the host. You then use these images to install guest operating systems on the new virtual machines.

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **Datastore browser**.
3. Select the datastore that you want to store the file on.
4. Optional: Click **Create directory** to create a new datastore directory to store the file.
5. Select the target folder and click **Upload**.
6. Locate the item that you want to upload from your local computer and click **Open**.
   The file uploads to the datastore that you selected.

7. Optional: Refresh the datastore file browser to see the uploaded file on the list.
8. Click **Close** to exit the file browser.

Download Files from a Datastore to Your System in the VMware Host Client

Use the datastore file browser to download files from the datastores available on the host that you are managing to your local system.

Required privilege: **Datastore** > **Browse Datastore**

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **Datastore browser**.
3. Select the target datastore.
4. Click the folder that contains the file that you want to download.
   The available files in the folder are displayed.
5. Click the file that you want to download.
6. Click **Download**.
   The file is downloaded to your system.
7. Click **Close** to exit the file browser.

Delete Files from a Datastore in the VMware Host Client

You can permanently remove files from any datastore if you no longer need them.

Required privilege: **Datastore** > **Browse Datastore**

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **Datastore browser**.
3. Select the target datastore.
4. Select the folder that contains the file that you want to delete.
   The available files in the folder are displayed.
5. Click the file that you want to remove from the datastore, click **Delete**, and click **Delete** again.
6. Click **Close** to exit the file browser.

Move Datastore Folders or Files in the VMware Host Client

Use the datastore file browser to move files or folders to a new location, either on the same datastore or on a different datastore.

Required privilege: **Datastore** > **Browse Datastore**

Note: Virtual disk files are moved and copied without format conversion. If you move a virtual disk to a datastore on a type of host that is different from the type of the source host, you might need to convert the virtual disks before you can use them.

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **Datastore browser**.
3. Select the target datastore.
4. Select the file or folder that you want to move to another location and click **Move**.
5. Select your target destination and click **Move**.
6. Click **Close** to exit the file browser.

Copy Datastore Folders or Files in the VMware Host Client

Use the datastore file browser to copy folders or files to a new location, either on the same datastore or on a different datastore.

Required privilege: **Datastore** > **Browse Datastore**

Note: Virtual disk files are moved and copied without format conversion. If you move a virtual disk to a datastore on a type of host that is different from the type of the source host, you might need to convert the virtual disks.

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **Datastore browser**.
3. Select the target datastore.
4. Select the file or folder that you want to move to another location and click **Copy**.
5. Select your target destination and click **Copy**.
6. Click **Close** to exit the file browser.

Create a New Datastore Directory in the VMware Host Client

You can create new datastore directories if you want to store files in a particular location.

Required privilege: **Datastore** > **Browse Datastore**

1. Click **Storage** in the inventory and click **Datastores**.
2. Click **Datastore browser**.
3. Click **Create directory**.
4. Select the target datastore.
5. Optional: Enter a name for the new directory.
6. Click **Create directory**.
7. Click **Close** to exit the file browser.

Rename a Datastore in the VMware Host Client

You can change the display name of a datastore in the VMware Host Client.

Note: If the host is managed by vCenter Server, you cannot rename the datastore from the VMware Host Client. You can only perform the task from the vCenter Server instance that manages the host.

1. Click **Storage** in the VMware Host Client inventory and click **Datastores**.
2. Right-click a datastore in the list and select **Rename** from the drop-down menu.
3. Enter a new name for the datastore and click **Save** to apply your changes.
4. Optional: Click **Refresh** to see the new name of the datastore in the list of available datastores.

Delete a VMFS Datastore in the VMware Host Client

You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, the datastore and all the files associated to the datastore are removed from the host.

Remove all virtual machines from the datastore.

Note: The datastore delete operation permanently deletes all files associated with virtual machines on the datastore. Although you can delete the datastore without unmounting, it is preferable that you unmount the datastore first.

1. Click **Storage** in the inventory and click **Datastores**.
2. Right-click the datastore from the list and select **Delete** from the drop-down menu.
3. Click **Confirm** to delete the datastore.

Storage Thin Provisioning in the VMware Host Client

With ESXi, you can use two models of thin provisioning, array-level and virtual-disk level thin provisioning.

Thin provisioning is a method that optimizes storage utilization by allocating storage space in a flexible on-demand manner. Thin provisioning contrasts with the traditional model, called thick provisioning. With thick provisioning, a large amount of storage space is provided in advance in anticipation of future storage needs. However, the space might remain unused causing underutilization of storage capacity.

The VMware thin provisioning features help you eliminate storage underutilization problems at the datastore and storage array level.

Create Thin Provisioned Virtual Disks in the VMware Host Client

To save storage space, you can create thin provisioned virtual disks. The thin provisioned virtual disk starts small and grows as more disk space is required. You can create thin disks only on the datastores that support disk-level thin provisioning.

The following procedure assumes that you are creating a new virtual machine. For more information, see Create a Virtual Machine in the VMware Host Client.

1. Right-click **Host** in the VMware Host Client inventory and select **Create/Register VM**.
   The **New Virtual Machine** wizard opens.
2. Select a method for adding a new virtual machine on the host and click **Next**.
3. Enter a name for your virtual machine.
4. Select the virtual machine compatibility from the **Compatibility** drop-down menu.
5. Select a guest operating system version from the **Guest OS version** drop-down menu and click **Next**.
6. From the list of accessible datastores on the Select storage page of the **New Virtual Machine** wizard, select the destination datastore for the virtual machine configuration files and all of the virtual disks.
7. On the **Virtual Hardware** tab, expand **Hard disk**.
8. Under **Disk Provisioning**, select the **Thin provisioned** radio button and click **Next**.
9. On the Ready to complete page of the **New Virtual Machine** wizard, review the configuration settings for the virtual machine and click **Finish** to save your settings.

View Virtual Machine Storage Resources in the VMware Host Client

You can view how datastore storage space is allocated for your virtual machines in the VMware Host Client.

Resource Consumption shows how much datastore space is occupied by virtual machine files, including configuration files, log files, snapshots, virtual disks, and so on. When the virtual machine is running, the used storage space also includes swap files.

For virtual machines with thin disks, the actual storage usage value might be less than the size of the virtual disk.

1. Click the virtual machine in the VMware Host Client inventory.
2. Review the Resource Consumption information in the lower right area of the virtual machine summary page.

Determine the Disk Format of a Virtual Machine in VMware Host Client

You can determine whether your virtual disk is provisioned in thick or thin format.

1. Right-click the virtual machine in the VMware Host Client inventory and select **Edit settings**.
2. On the **Virtual Hardware** tab, expand **Hard disk**.
   The **Type** text box shows the format of your virtual disk.

Managing Storage Adapters in the VMware Host Client

When you connect to a host or to vCenter Server by using the VMware Host Client, you can perform various tasks on your storage adapters, such as configuring various iSCSI components.

When you enable iSCSI on the host that you are managing in your VMware Host Client environment, you can configure and add new network port bindings, static and dynamic targets, you can manage CHAP authentication, and configure various advanced settings on your host storage.

View Storage Adapters in the VMware Host Client

View the storage adapters that your host uses and related information.

1. Click **Storage** in the VMware Host Client inventory and click **Adapters**.
   All storage adapters available to the host are listed under **Adapters**.
2. To view details for a specific adapter, select the adapter from the list.

Configuring Software iSCSI Adapters in the VMware Host Client

With the software-based iSCSI implementation, you can use standard NICs to connect your host to a remote iSCSI target on the IP network. The software iSCSI adapter that is built into ESXi communicates with the physical NICs through the network stack.

Note: Before you can use the software iSCSI adapter, you must set up networking, activate the adapter, and configure parameters such as CHAP.

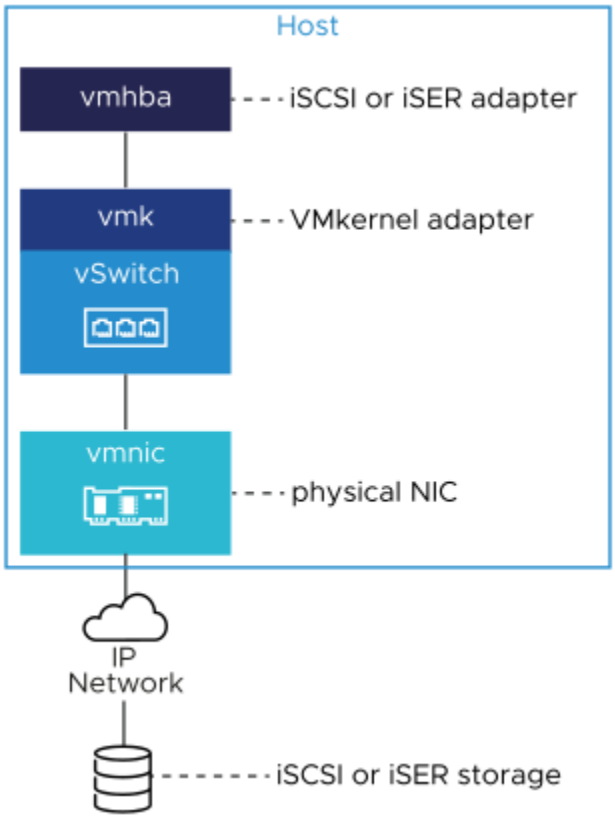
The iSCSI adapter configuration workflow includes the following procedures:

- Enabling iSCSI on your host. SeeEnable iSCSI for an ESXi Host in the VMware Host Client.
- Adding a port binding. See Add Port Binding in the VMware Host Client.
- Removing port binding. See Remove Port Binding in the VMware Host Client.

Setting Up Network for iSCSI and iSER

Certain types of iSCSI adapters depend on the VMkernel networking. These adapters include the software or dependent hardware iSCSI adapters, and the VMware iSCSI over RDMA (iSER) adapter. If your environment includes any of these adapters, you must configure connections for the traffic between the iSCSI or iSER component and the physical network adapters.

Configuring the network connection involves creating a virtual VMkernel adapter for each physical network adapter. You use 1:1 mapping between each virtual and physical network adapter. You then associate the VMkernel adapter with an appropriate iSCSI or iSER adapter. This process is called port binding.



Follow these rules when configuring the port binding:

- You can connect the software iSCSI adapter with any physical NICs available on your host.
- The dependent iSCSI adapters must be connected only to their own physical NICs.
- You must connect the iSER adapter only to the RDMA-capable network adapter.

For specific considerations on when and how to use network connections with software iSCSI, see the VMware knowledge base article at http://kb.vmware.com/kb/2038869.

Enable iSCSI for an ESXi Host in the VMware Host Client

Enable iSCSI for your host in your VMware Host Client environment to configure storage adapters parameters, such as CHAP authentication, network port bindings, static and dynamic targets, and various advanced settings.

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. Select the **Enabled** radio button.
3. Optional: Configure the parameters and components that you want to change.
4. Click **Save configuration**.

Best Practices for Configuring Networking with Software iSCSI

When you configure networking with software iSCSI, consider several best practices.

Software iSCSI Port Binding

You can bind the software iSCSI initiator on the ESXi host to a single or multiple VMkernel ports, so that iSCSI traffic flows only through the bound ports. Unbound ports are not used for iSCSI traffic.

When port binding is configured, the iSCSI initiator creates iSCSI sessions from all bound ports to all configured target portals.

See the following examples.

VMkernel Ports	Target Portals	iSCSI Sessions
2 bound VMkernel ports	2 target portals	4 sessions (2 x 2)
4 bound VMkernel ports	1 target portal	4 sessions (4 x 1)
2 bound VMkernel ports	4 target portals	8 sessions (2 x 4)

Note: Make sure that all target portals are reachable from all VMkernel ports when port binding is used. Otherwise, iSCSI sessions might fail to create. As a result, the rescan operation might take longer than expected.

No Port Binding

If you do not use port binding, the ESXi networking layer selects the best VMkernel port based on its routing table. The host uses the port to create an iSCSI session with the target portal. Without the port binding, only one session per each target portal is created.

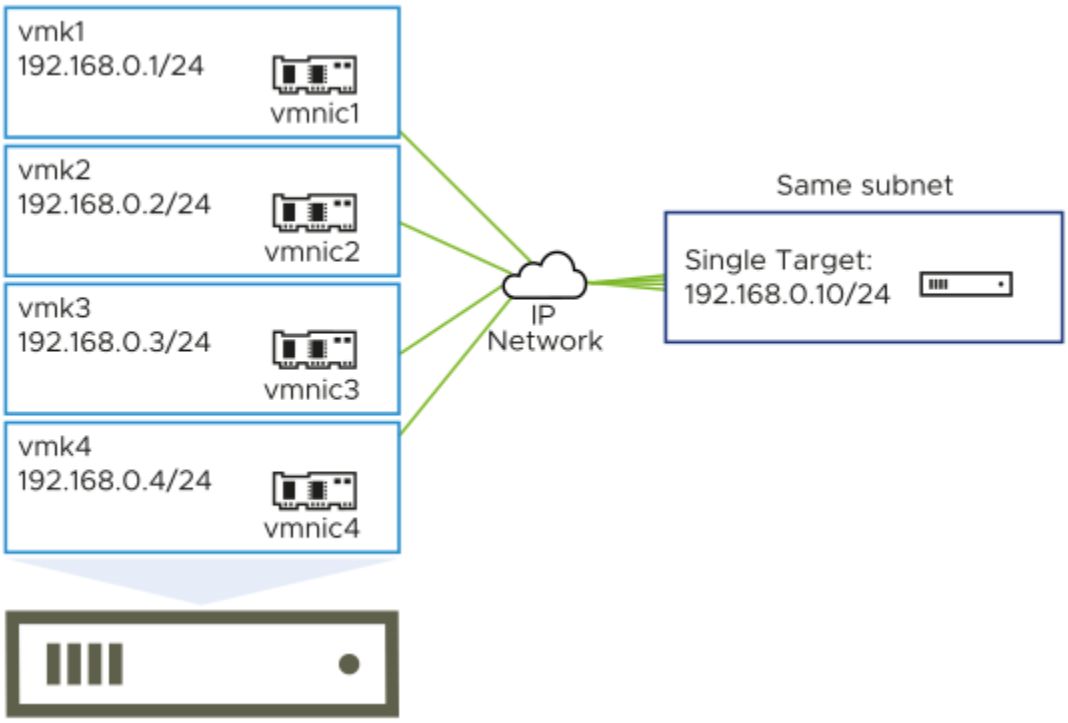
See the following examples.

VMkernel Ports	Target Portals	iSCSI Sessions
2 unbound VMkernel ports	2 target portals	2 sessions
4 unbound VMkernel ports	1 target portal	1 session
2 unbound VMkernel ports	4 target portals	4 sessions

Software iSCSI Multipathing

Example 1. Multiple paths for an iSCSI target with a single network portal

If your target has only one network portal, you can create multiple paths to the target by adding multiple VMkernel ports on your ESXi host and binding them to the iSCSI initiator.

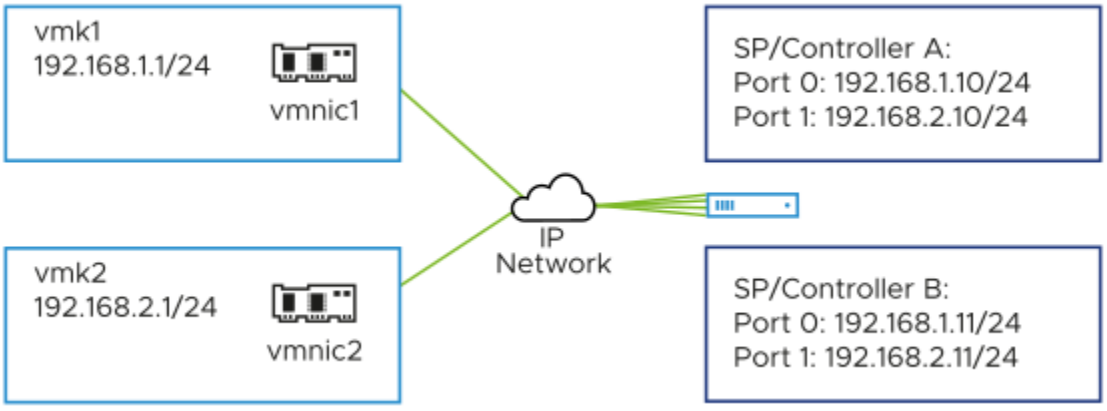


In this example, all initiator ports and the target portal are configured in the same subnet. The target is reachable through all bound ports. You have four VMkernel ports and one target portal, so total of four paths are created.

Without the port binding, only one path is created.

Example 2. Multiple paths with VMkernel ports in different subnets

You can create multiple paths by configuring multiple ports and target portals on different IP subnets. By keeping initiator and target ports in different subnets, you can force ESXi to create paths through specific ports. In this configuration, you do not use port binding because port binding requires that all initiator and target ports are on the same subnet.



ESXi selects vmk1 when connecting to Port 0 of Controller A and Controller B because all three ports are on the same subnet. Similarly, vmk2 is selected when connecting to Port 1 of Controller A and B. You can use NIC teaming in this configuration.

Total of four paths are created.

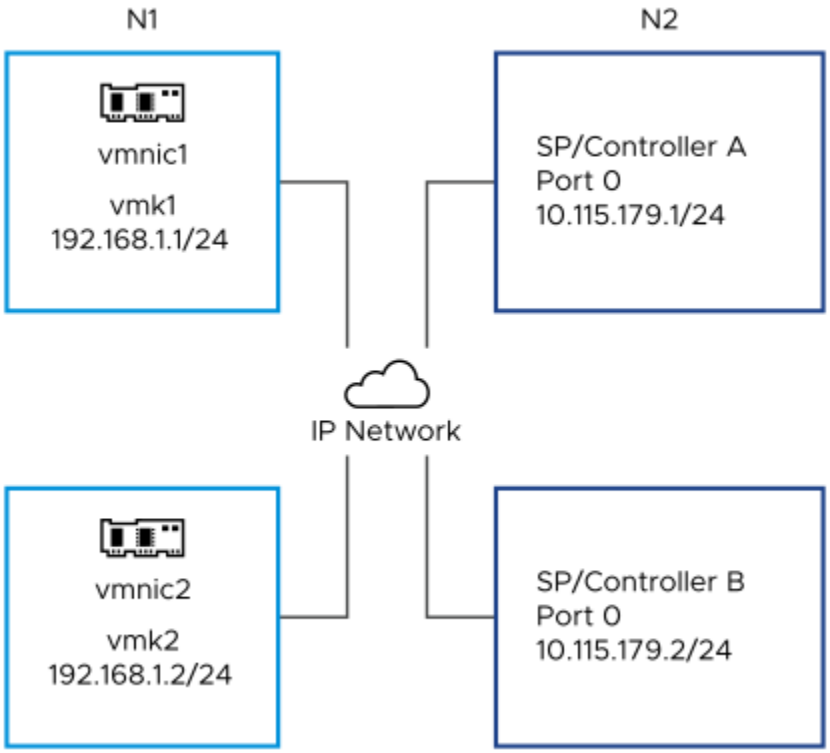
Paths	Description
Path 1	vmk1 and Port0 of Controller A
Path 2	vmk1 and Port0 of Controller B
Path 3	vmk2 and Port1 of Controller A
Path 4	vmk2 and Port1 of Controller B

Routing with Software iSCSI

You can use the `esxcli` command to add static routes for your iSCSI traffic. After you configure static routes, initiator and target ports in different subnets can communicate with each other.

Example 1. Using static routes with port binding

In this example, you keep all bound VMkernel ports in one subnet (N1) and configure all target portals in another subnet (N2). You can then add a static route for the target subnet (N2).

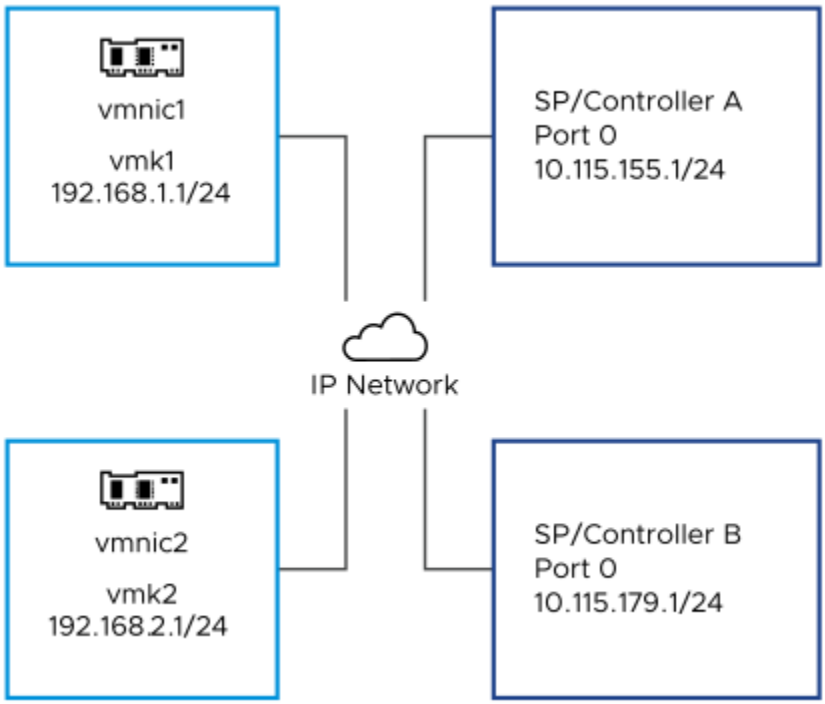


Use the following command:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.179.0/24
```

Example 2. Using static routes to create multiple paths

In this configuration, you use static routing when using different subnets. You cannot use the port binding with this configuration.



You configure vmk1 and vmk2 in separate subnets, 192.168.1.0 and 192.168.2.0. Your target portals are also in separate subnets, 10.115.155.0 and 10.155.179.0.

You can add the static route for 10.115.155.0 from vmk1. Make sure that the gateway is reachable from vmk1.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24
```

You then add static route for 10.115.179.0 from vmk2. Make sure that the gateway is reachable from vmk2.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24
```

When connecting with Port 0 of Controller A, vmk1 is used.

When connecting with Port 0 of Controller B, vmk2 is used.

Example 3. Routing with a separate gateway per vmkernel port

Starting with vSphere 6.5, you can configure a separate gateway per VMkernel port. If you use DHCP to obtain IP configuration for a VMkernel port, gateway information can also be obtained using DHCP.

To see gateway information per VMkernel port, use the following command:

```
# esxcli network ip interface ipv4 address list
 Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
 ----  --------------  -------------  --------------  ------------  --------------  --------
 vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
 vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
 vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

With separate gateways per VMkernel port, you use port binding to reach targets in different subnets.

Add Port Binding in the VMware Host Client

Use the VMware Host Client to bind an iSCSI adapter with a VMkernel adapter on your host.

- Create a virtual VMkernel adapter for each physical network adapter on your host. If you use multiple VMkernel adapters, set up the correct network policy.
- Required privilege:**Host** > **Configuration** > **Storage Partition Configuration**

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. In the **Network port bindings** section, click **Add port binding**.
3. Select a VMkernel adapter to bind with the iSCSI adapter.

   Note: Make sure that the network policy for the VMkernel adapter is compliant with the binding requirements.

   You can bind the software iSCSI adapter to one or more VMkernel adapters. For a dependent hardware iSCSI adapter, only one VMkernel adapter associated with the correct physical NIC is available.
4. Click **Select**.
5. Click **Save configuration**.

Remove Port Binding in the VMware Host Client

Edit the iSCSI configuration on your host to remove a port binding.

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. In the **Network port bindings** section, select a VMkernel NIC from the list.
3. Click **Remove port binding**.
4. Click **Save configuration**.

Set up a Dynamic Target in the VMware Host Client

With Dynamic Discovery, each time the initiator contacts a particular iSCSI storage system, the initiator sends the SendTargets request to the iSCSI system. The iSCSI system responds by supplying a list of available targets to the initiator.

Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

When you set up Dynamic Discovery, you can only add a new iSCSI system. You cannot change the IP address, DNS name, or port number of an existing iSCSI system. To modify the parameters, delete the existing system and add a new one.

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. Click **Add dynamic target**.

   The new dynamic target appears in the list.
3. To add an address for the new dynamic target, click the target in the list and enter the address .
4. Optional: To change the port number of the new dynamic target, click the target **Port** text box and enter the new port number.
5. Optional: To edit the dynamic target settings, select the new target from the list of available targets, click **Edit settings**, configure the parameters that you want to change, and click **Save**.
6. Optional: To delete a specific target, select the target and click **Remove dynamic target**.

   The target no longer appears in the list of existing dynamic targets.

7. Click **Save configuration**.

Set Up a Static Target in the VMware Host Client

With iSCSI initiators, you can use static discovery to manually enter information for the targets.

Required privileges: **Host** > **Configuration** > **Storage Partition Configuration**

When you set up Static Discovery, you can only add new iSCSI targets. You cannot change the IP address, DNS name, iSCSI target name, or port number of an existing target. To make changes, remove the existing target and add a new one.

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. Click **Add static target**.
   The new static target appears in the list.
3. To add a name for the new static target, click the target in the list and enter the name.
4. To add an address for the new static target, click the target in the list and type the address.
5. Optional: To change the port number of the new static target, click the target **Port** text box and type the new port number.
6. Optional: To edit the static target settings, select the new target from the list of available targets, click **Edit settings**, configure the parameters that you want to change, and click **Save**.
7. Optional: To delete a specific target, select the target and click **Remove static target**.
   The target no longer appears in the list of existing static targets.
8. Click **Save configuration**.

Edit Advanced Settings for iSCSI in the VMware Host Client

The advanced iSCSI settings control such parameters as header and data digest, ARP redirection, delayed ACK, and so on. Generally, you do not need to change these settings because your host works with the assigned predefined values.

Required privilege: **Host** > **Configuration** > **Storage Partition Configuration**

CAUTION: Do not change the advanced iSCSI settings unless you are working with the VMware support team or otherwise have thorough information about the values to provide for the settings modification.

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. Click **Advanced settings** to display the entire list of settings.
3. Edit the parameters that you want to change and click **Save configuration**.

Set Up CHAP Authentication for an iSCSI Adapter in the VMware Host Client

You can set up all targets to receive the same CHAP name and secret from the iSCSI initiator at the initiator level. By default, all discovery addresses or static targets inherit the CHAP parameters that you set up at the initiator level.

- Before you set up CHAP parameters for software or dependent hardware iSCSI, determine whether to configure one-way, also known as normal, or mutual CHAP. Independent hardware iSCSI adapters do not support mutual CHAP.
  - In one-way CHAP, the target authenticates the initiator.
  - In mutual CHAP, both the target and the initiator authenticate each other. Use different secrets for CHAP and mutual CHAP.

  When you configure CHAP parameters, verify that they match the parameters on the storage side.

- Required privileges: **Host** > **Configuration** > **Storage Partition Configuration**

The CHAP name must be fewer than 511 alphanumeric characters and the CHAP secret must be fewer than 255 alphanumeric characters. Some adapters, for example the QLogic adapter, might have lower limits, 255 for the CHAP name and 100 for the CHAP secret.

1. Click **Storage** in the inventory, click **Adapters**, and click **Configure iSCSI**.
2. To configure one-way CHAP, expand **CHAP authentication** to display all parameters.
   a) Select the CHAP security level.
   b) Enter the CHAP name.

      Make sure that the name you enter matches the name configured on the storage side.
   c) Enter a one-way CHAP secret to use for authentication. Use the same secret that you enter on the storage side.
3. To configure mutual CHAP, select **Use CHAP** as an option for one-way CHAP. Expand **Mutual CHAP authentication** to display all parameters.
   a) Select **Use CHAP**.
   b) Enter the mutual CHAP name.
   c) Enter the mutual CHAP secret.

      Use different secrets for the one-way CHAP and the mutual CHAP.
4. Click **Save configuration**.

If you change the authentication settings for an iSCSI adapter, you only use the updated credentials for new iSCSI sessions. Existing sessions persist until either the connection is lost due to some outside factor, such as force re-authentication, or you remove and add the adapter iSCSI targets.

Managing Storage Devices in the VMware Host Client

You can use the VMware Host Client to manage local and networked storage devices that the ESXi host you are managing has access to.

View Storage Devices in the VMware Host Client

View all storage devices available to a host. If you use third-party multipathing plug-ins, the storage devices available through the plug-ins also appear on the list.

The Storage Devices view allows you to list the host storage devices, analyze their information, and modify properties.

1. Click **Storage** in the VMware Host Client inventory and click **Devices**.

   All storage devices available to the host are listed under **Devices**.
2. To view details for a specific device, select the device from the list.

Clear a Device Partition Table in theVMware Host Client

When you are logged in to anESXi host with theVMware Host Client, you can clear the partition table of a disk device that is accessible from the host.

Verify that the device is not in use byESXi as boot disk, VMFS datastore, or vSAN.

1. Click **Storage** in theVMware Host Client and click **Devices**.
2. Right-click a device from the list, click **Clear partition table** and click **Yes**.

   Clearing the partition table might cause data loss.

Edit Individual Device Partitions in theVMware Host Client

When you log in to anESXi host with theVMware Host Client, you can remove individual partitions of a device by using the partition editor

Verify that the device is not in use byESXi as boot disk, VMFS datastore, or vSAN.

1. Click **Storage** in theVMware Host Client and click **Devices**.
2. Right-click a device from the list and click **Edit partitions**.
3. Select a partition and click **Delete partition**.
4. Optional: Click **Reset** to restore the original partitions.
5. Click **Save partitions**.
6. Confirm that you want to alter the partition.

Managing Persistent Memory

ESXi6.7 provides support for the latest computer memory technology, which is called non-volatile memory (NVM) or persistent memory (PMem). PMem combines the high data transfer rate of volatile computer memory with the persistence and resiliency of traditional storage. PMem devices have low access latency and can retain stored data through reboots or power outages.

Modes of Consumption of the Persistent Memory Resources of the Host

When you add a physical PMem device to a host, ESXi detects the PMem resource and exposes it as a host-local PMem datastore to the virtual machines that run on the host. Depending on the guest operating system, virtual machines can have direct access to the PMem resources.

Each host can have only one local PMem datastore that pools and represents all PMem resources of the host.

Persistent memory combines the properties of both memory and storage. So, virtual machines can consume the PMem resources of the ESXi host as memory (through virtual NVDIMM devices) or as storage (through virtual PMem hard disks).

The host-local PMem datastore stores all direct-accessed NVDIMM devices and virtual PMem hard disks.

Virtual PMem (vPMem)

In this mode, if the guest operating system is PMem-aware, the virtual machine can have direct access to the physical PMem resources of the host and use them as standard, byte-addressable memory.

Virtual machines use virtual non-volatile dual in-line memory modules (NVDIMMs) for direct access to PMem. The NVDIMM is a memory device that sits on an ordinary memory channel, but contains non-volatile memory. In vSphere 6.7, the virtual NVDIMM is a new type of device that represents the physical PMem regions of the host. A single virtual machine can have up to 64 virtual NVDIMM devices. Each NVDIMM device is stored on the host-local PMem datastore.

Note: To add an NVDIMM device to a virtual machine, the virtual machine must be of hardware version 14 and the guest operating system must support persistent memory. If the guest operating system is not PMem-aware, you can still use PMem, but you cannot add an NVDIMM device to the virtual machine.

Virtual PMem Disks (vPMemDisk)

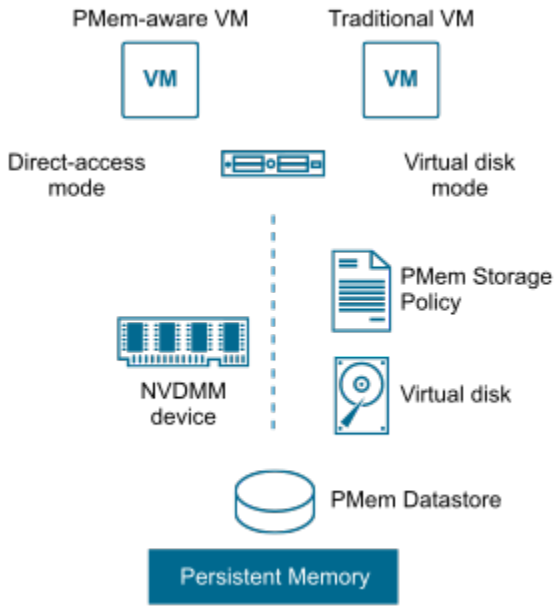
In this mode, the virtual machine does not have direct access to the PMem resources of the host.

You must add a virtual PMem hard disk to the virtual machine. A virtual PMem hard disk is a traditional SCSI disk to which the PMem Storage Policy is applied. The policy automatically places the hard disk on the host-local PMem datastore.

In this mode of usage, there are no requirements for the hardware version of the virtual machine and the guest operating system.

Note: If the guest operating system is not PMem-aware, virtual machines can use PMem only through vPMemDisks.

The following diagram illustrates how the persistent memory components interact.



For information about how to configure and manage VMs with NVDIMMs or virtual persistent memory disks, see the *vSphere Resource Management* documentation.

Structure of the PMem Datastore

The VMware Host Client user interface provides information about the complex structure of the host-local PMem datastore. To analyze this information and use it for troubleshooting and management purposes, you must be familiar with the concepts related to that complex structure.

Modules	In the VMware Host Client user interface, modules represent the physical NVDIMMs that are connected to the motherboard of the host. In the VMware Host Client, you can check the health status of each module and identify unhealthy NVDIMM modules.
Interleave Sets	Interleave sets are logical groupings of one or multiple modules. Interleave sets reveal how information is spread across the physical DIMMs and how ESXi reads the information from the modules. Because ESXi reads from each interleave set in turns, interleave sets ensure higher memory throughput. For example, if an interleave set consists of two modules, ESXi reads the information from the two physical DIMMs in parallel and then proceeds with the next interleave set. The VMware Host Client user interface provides information about the way NVDIMMs are grouped into interleave sets.

Namespaces	Namespaces are regions of contiguously addressed memory ranges in the NVDIMM. Namespaces can go across interleave sets. The PMem datastore is built on top of the namespaces. In the VMware Host Client, you can view the capacity, health status, and the location ID of every namespace.

View Information About Modules, Interleave Sets, and Namespaces in the VMware Host Client

In the VMware Host Client you can view information about the modules, interleave sets, and namespace of the host-local PMem datastore. As a result, you can easily identify an unhealthy module and perform troubleshooting.

Verify that the host has at least one physical NVDIMM device.

You cannot perform most of the traditional datastore management tasks on the host-local PMem datastore. However, you can use the information about modules, interleave sets, and namespaces for troubleshooting purposes.

1. In the **Navigator** pane, click **Storage**.
2. On the **Persistent Memory** tab, view information about the host-local PMem datastore.
   - Click **Modules** to view information about the NVDIMMs that make up the PMem datastore.
   - Click **Namespaces** to view information about namespaces on the NVDIMMs.
   - Click **Interleave sets** to see how the modules, or physical NVDIMMs, are grouped into interleave sets.

Delete a Namespace in the VMware Host Client

In the VMware Host Client, you can delete namespaces that were not created by ESXi, but by an OS that was previously installed on the host machine.

- Put the host in maintenance mode.
- Back up the content of the namespace if you might need that content at a later time.

1. In the VMware Host Client, click **Storage**.
2. Under the **Persistent Memory** tab, click **Namespaces**.
3. Optional: In the list of namespaces, check the State column to determine which namespaces ESXi currently uses.
   To free up space, you must delete namespaces whose state is In Use.
4. Select a namespace and click the **Delete** icon.

   Important: Deleting a namespace frees up space on the datastore, but you can use the free space only after you reboot the host.
5. Click the **Reboot host** icon to reboot the host.

The selected namespace is deleted from the PMem datastore. ESXi automatically creates a new namespace that the PMem datastore can use. The new namespace has the same capacity, type, and location ID as the deleted one.

Monitoring Storage in the VMware Host Client

In the VMware Host Client, you can monitor the storage health of the ESXi host that you are managing. You can also view events and tasks associated with the different datastores, storage adapters, and storage devices on the host that you are managing.

Monitor Datastores in the VMware Host Client

In the VMware Host Client, you can monitor the health of a datastore, and events and tasks associated with that datastore. Starting with vSphere 6.5 Update 1 and after you enable the vSAN service in the vSphere Client, you can also monitor your vSAN environment.

1. Click **Storage** in the inventory.
2. Click **Datastores**.
3. Click a datastore from the list.
   The datastore expands in the VMware Host Client inventory.
4. Click **Monitor** under the name of the datastore.
5. Optional: Click **Events** to view events associated with the datastore.
6. Optional: Click **vSAN** to view the configuration parameters of the vSAN environment of your host.
7. Optional: Click **Hosts** to view the hosts that reside on this datastore.
8. Optional: Click **Health** to view details about the status of various parameters, such as **Performance service**, **Network**, **Physical disk**, **Data**, **Cluster**, and **Limits**.

Monitoring vSAN in the VMware Host Client

You can use the VMware Host Client to monitor the vSAN environment of your ESXi host.

vSAN Concepts

VMware vSAN uses a software-defined approach that creates shared storage for virtual machines. It virtualizes the local physical storage resources of ESXi hosts. It also turns them into pools of storage that can be divided and assigned to virtual machines and applications according to their quality-of-service requirements. vSAN is implemented directly in the ESXi hypervisor.

You can configure vSAN to work as either a hybrid or all-flash cluster. In hybrid clusters, flash devices are used for the cache layer and magnetic disks are used for the storage capacity layer. In all-flash clusters, flash devices are used for both cache and capacity.

You can activate vSAN on your existing host clusters and when you create clusters.

If vSAN is set to Auto mode, vSAN aggregates all free local capacity devices into a single datastore shared by all hosts in the vSAN cluster. vSAN cannot use devices that are formatted and already contain some information.

If vSAN is set to Manual mode, vSAN uses the local capacity devices that you claimed by using the vSphere Client. If you did not claim any devices through the vSphere Client, your vSAN datastore size is 0 MB.

You can expand the datastore by adding capacity devices or hosts with capacity devices to the cluster. vSAN works best when all ESXi hosts in the cluster share similar or identical configurations across all cluster members, including similar or identical storage configurations. This consistent configuration balances virtual machine storage components across all devices and hosts in the cluster. Hosts without any local devices also can participate and run their virtual machines on the vSAN datastore.

If a host contributes its local storage devices to the vSAN datastore, it must provide at least one device for flash cache and at least one device for capacity. Capacity devices are also called data disks.

The devices on the contributing host form one or more disk groups. Each disk group contains one flash cache device, and one or multiple capacity devices for persistent storage. Each host can be configured to use multiple disk groups.

For best practices, capacity considerations, and general recommendations about designing and sizing a vSAN cluster, see the *VMware vSAN Design and Sizing Guide*.

Characteristics of vSAN

This topic summarizes characteristics that apply to vSAN, its clusters, and datastores.

vSAN provides numerous benefits to your environment.

Table 529: vSAN Features

Supported Features	Description
Shared storage support	vSAN supports VMware features that require shared storage, such as HA, vMotion, and DRS. For example, if a host becomes overloaded, DRS can migrate virtual machines to other hosts in the cluster.
On-disk format	vSAN on-disk virtual file format provides highly scalable snapshot and clone management support per vSAN cluster. For information about the number of virtual machine snapshots and clones supported per vSAN cluster, see the *Configuration Maximums* documentation.
All-flash and hybrid configurations	vSAN can be configured for all-flash or hybrid cluster.
Fault domains	vSAN supports configuring fault domains to protect hosts from rack or chassis failures when the vSAN cluster spans across multiple racks or blade server chassis in a data center.
iSCSI target service	vSAN iSCSI target service enables hosts and physical workloads that reside outside the vSAN cluster to access the vSAN datastore.
Stretched cluster	vSAN supports stretched clusters that span across two geographic locations.
Support for Windows Server Failover Clusters (WSFC)	vSAN 6.7 Update 3 and later releases support SCSI-3 Persistent Reservations (SCSI3-PR) on a virtual disk level required by Windows Server Failover Cluster (WSFC) to arbitrate an access to a shared disk between nodes. Support of SCSI-3 PRs enables configuration of WSFC with a disk resource shared between VMs natively on vSAN datastores. Currently the following configurations are supported: • Up to 6 application nodes per cluster. • Up to 64 shared virtual disks per node. **Note:** Microsoft SQL Server 2012 or later running on Microsoft Windows Server 2012 or later has been qualified on vSAN.
vSAN health service	vSAN health service includes preconfigured health check tests to monitor, troubleshoot, diagnose the cause of cluster component problems, and identify any potential risk.
vSAN performance service	vSAN performance service includes statistical charts used to monitor IOPS, throughput, latency, and congestion. You can monitor performance of a vSAN cluster, host, disk group, disk, and VMs.
Integration with vSphere storage features	vSAN integrates with vSphere data management features traditionally used with VMFS and NFS storage. These features include snapshots, linked clones, and vSphere Replication.
Virtual Machine Storage Policies	vSAN works with VM storage policies to support a VM-centric approach to storage management. If you do not assign a storage policy to the virtual machine during deployment, the vSAN Default Storage Policy is automatically assigned to the VM.

Supported Features	Description
Rapid provisioning	vSAN enables rapid provisioning of storage in the vCenter Server® during virtual machine creation and deployment operations.
Deduplication and compression	vSAN performs block-level deduplication and compression to save storage space. When you enable deduplication and compression on a vSAN all-flash cluster, redundant data within each disk group is reduced. Deduplication and compression is a cluster-wide setting, but the functions are applied on a disk group basis. Compression-only vSAN is applied on a per-disk basis.
Data at rest encryption	vSAN provides data at rest encryption. Data is encrypted after all other processing, such as deduplication, is performed. Data at rest encryption protects data on storage devices, in case a device is removed from the cluster.
SDK support	The VMware vSAN SDK for Java is an extension of the VMware vSphere Management SDK. It includes documentation, libraries and code examples that help developers automate installation, configuration, monitoring, and troubleshooting of vSAN.

Monitor vSAN in the VMware Host Client

You can use the VMware Host Client to monitor the vSAN environment of your ESXi host.

vSAN service must be enabled in the vSphere Client before you can view the vSAN related screens for a datastore.

1. Click **Storage** in the inventory.
2. On the **Datastores** tab, click **vSAN Datastore**.
   The vSAN Datastore expands in the VMware Host Client navigator.
3. Click **Monitor**.
   You are present with the **vSAN**, **Host**, and **Health** tabs in the UI.

Option	Description
vSAN	Displays the configurations for the current host. You can edit the settings for the claiming mode and deduplication. You can also view the settings for: • Encryption – vSAN supports encryption of the information for the whole vSAN datastore. • ISCSI Service – Additional service through the iSCSI service. • Performance Service - Collects data on how the datastore works. For example, the speed of a read/write operation.
Hosts	Displays a list of all the hosts on the vSAN server with their IP and the fault domain they belong to.
Health	The **Health** tab contains tests organized in groups. You are present with the following groups: • Performance Service • Network • Physical disk • Data • Cluster

Option	Description
	• Limits Each group is labeled with a status icon for an error, warning, unknown or healthy. The status of the group represents the most severe state of the test belonging to that group. To view the tests and their descriptions, click the expand icon in the top right corner of the group of interest. From the expanded card you can review all the tests belonging to the group, the result of their execution and get more information about what each test examines on the system.

4. Select the vSAN parameter that you want to monitor.

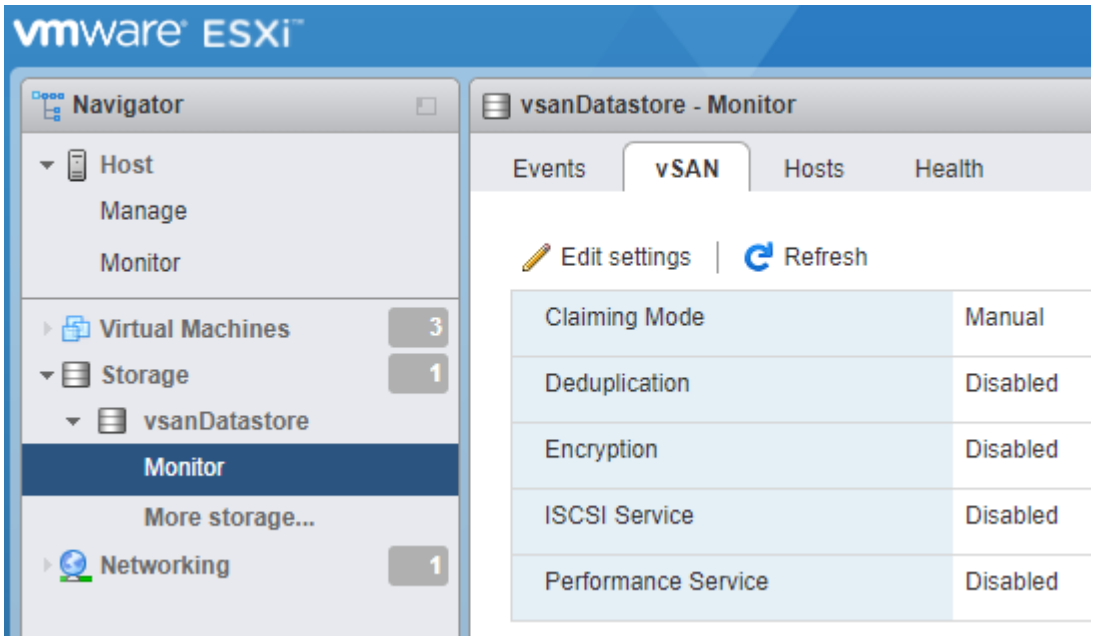
Edit Settings for a vSAN Datastore

You can edit the settings for a vSAN datastore when you must exit from a misconfigured state of the current host.

You can only edit the **Claiming Mode** and **Deduplication** settings for a vSAN datastore. These changes take effect only on the current host. They are not synced to the other hosts participating into the vSAN cluster.

Note: Only use these settings for troubleshooting.

1. Click **Storage** in the inventory.
2. On the **Datastores** tab, click a vSAN datastore from the table.
3. Click **Monitor** and click the **vSAN** tab.



4. Click **Edit settings**.
   The **Edit Settings** dialog box opens.
5. Change the settings.Select **Auto** or **Manual** from the **Claiming Mode**.

Option	Action
Claiming Mode	1. Select **Auto** or **Manual** from the **Claiming Mode**.

Option	Action
	– If you select **Auto**, it automatically takes all disks and claims them in a group or groups of the same size. **Note:** The **Auto** mode is deprecated. It can only claim hybrid disk groups which are not compatible with most of the vSAN features. – If you select **Manual**, you must manually organize the disks in groups and reclaim them by using the vSphere Web Client. For instance, selecting manual claiming mode is appropriate when the vCenter Server is unavailable.
Deduplication	1. Select **Enabled** or **Disabled** for the **Deduplication**.

6. Click **Save**.

Performing Storage Refresh and Rescan Operations in the VMware Host Client

The refresh operation for datastores, storage devices, and storage adapters updates the lists and storage information that the VMware Host Client displays. It updates information such as the datastore capacity. When you perform storage management tasks or make changes in the SAN configuration, you might need to rescan your storage.

Perform Adapter Rescan in the VMware Host Client

When you make changes in your SAN configuration and these changes are isolated to storage accessed through a specific adapter, perform rescan for only this adapter. When you rescan an adapter, you discover any new LUNs that are available on that adapter.

1. Click **Storage** in the VMware Host Client inventory and click **Adapters**.
2. Click **Rescan**.

Perform Device Rescan in the VMware Host Client

When you rescan a device, you discover any new VMFS volumes that are available on the device.

1. Click **Storage** in the VMware Host Client inventory and click **Devices**.
2. Click **Rescan**.

Change the Number of Scanned Storage Devices in the VMware Host Client

The range of scanned LUN IDs for an ESXi host can be from 0 to 16,383. ESXi ignores LUN IDs greater than 16,383. The configurable `Disk.MaxLUN` parameter controls the range of scanned LUN ID range. The parameter has a default value of 1024.

The `Disk.MaxLUN` parameter also determines how many LUNs the SCSI scan code attempts to discover using individual INQUIRY commands if the SCSI target does not support direct discovery using REPORT_LUNS.

You can modify the `Disk.MaxLUN` parameter depending on your needs. For example, if your environment has a smaller number of storage devices with LUN IDs from 1 through 100, set the value to 101. As a result, you can improve device discovery speed on targets that do not support REPORT_LUNS. Lowering the value can shorten the rescan time and boot time. However, the time to rescan storage devices might also depend on other factors, including the type of the storage system and the load on the storage system.

In other cases, you might need to increase the value if your environment uses LUN IDs that are greater than 1023.

1. Click **Manage** in the VMware Host Client inventory and click **Advanced Settings**.
2. Scroll down to `Disk.MaxLUN`.
3. Right-click `Disk.MaxLUN`, and click **Edit option**.
4. Enter a new value and click **Save**.
   The SCSI scan code does not scan the LUNs with IDs greater than or equal to the value you enter.
   For example, to discover LUN IDs from 0 to 100, set `Disk.MaxLUN` to 101.

Networking in the VMware Host Client

When you connect to an ESXi host using the VMware Host Client, you can view and configure vSphere standard switches, port groups, physical NICs, VMkernel NICs, and TCP/IP stacks.

Managing Port Groups in the VMware Host Client

You can manage port group settings to configure traffic management, enhance networking security, and enhance performance. By using the VMware Host Client, you can add and remove port groups. You can also examine port group information and edit port group settings, such as NIC teaming and traffic shaping.

View Port Group Information in the VMware Host Client

In the VMware Host Client, you can view information about port group configuration, network details, virtual switch topology, NIC teaming policy, offload policy, and security policy.

1. Click **Networking** in the VMware Host Client inventory and click **Port groups**.
2. Click an item from the list of available port groups.
   Information about network details, virtual switch topology, NIC teaming policy, offload policy, and security policy is displayed.

Add a Virtual Switch Port Group in the VMware Host Client

You can add a port group to a virtual switch in the VMware Host Client. Port groups provide networking for virtual machines.

1. Right-click **Networking** in the VMware Host Client inventory and click **Add port group** from the pop-up menu.
2. Enter a name for the new port group.
3. Set the VLAN ID to configure VLAN handling in the port group.
   The VLAN ID also reflects the VLAN tagging mode in the port group.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN.
Virtual Switch Tagging (VST)	From 1 to 4094	The virtual switch tags traffic with the tag that you entered.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch permits traffic from any VLAN.

4. Select a virtual switch from the drop-down menu.
5. Expand **Security** and select options that you want to enable for promiscuous mode, MAC address changes, and forged transmits.
6. Click **Add**.
   Your port group is created.
7. Optional: Click **Refresh** to display the new port group in the list.

Edit Port Group Settings in theVMware Host Client

To enhance networking security and improve networking performance in theVMware Host Client, you can edit various port group settings, such as the port group name, VLAN ID, and virtual switch. You can also configure security, NIC teaming, and traffic shaping components.

1. Click **Networking** in theVMware Host Client inventory and click **Port groups**.
2. Right-click the port group in the list that you want to edit and select **Edit settings**.
3. Optional: Enter a new port group name.
4. Optional: Enter a new value for the VLAN ID.
   The VLAN ID reflects the VLAN tagging mode in the port group.

VLAN Tagging Mode	VLAN ID	Description
External Switch Tagging (EST)	0	The virtual switch does not pass traffic associated with a VLAN.
Virtual Switch Tagging (VST)	From 1 to 4094	The virtual switch tags traffic with the tag that you entered.
Virtual Guest Tagging (VGT)	4095	Virtual machines handle VLANs. The virtual switch permits traffic from any VLAN.

5. Optional: Select a virtual switch from the drop-down menu.
6. Optional: Expand **Security** and select whether to reject, accept, or inherit the Security policy exceptions from vSwitch.

Option	Description
Promiscuous Mode	• **Reject**. Placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter. • **Accept**. Placing a guest adapter in promiscuous mode causes it to detect all frames passed on the vSphere distributed switch that are allowed under the VLAN policy for the port group that the adapter is connected to. • **Inherit from vSwitch**. Placing a guest adapter in promiscuous mode causes it to inherit the configuration from the associated virtual switch.
MAC Address Changes	• **Reject**. If you set the **MAC Address Changes** to **Reject** and the guest operating system changes the MAC address of the adapter to anything other than what is in the `.vmx` configuration file, all inbound frames are dropped. If the guest operating system changes back the MAC address to match the MAC address in the `.vmx` configuration file, inbound frames are passed again.

Option	Description
	• **Accept**. Changing the MAC address from the guest operating system has the intended effect: frames to the new MAC address are received. • **Inherit from vSwitch**. If you set **MAC Address Changes** to **Inherit from vSwitch**, the MAC address changes to one of the associated virtual switches.
Forged Transmits	• **Reject**. Any outbound frame with a source MAC address that is different from the one set on the adapter are dropped. • **Accept**. No filtering is performed and all outbound frames are passed. • **Inherit from vSwitch**. The outbound frame configuration is inherited from the associated virtual switch.

7. Optional: Expand **NIC teaming** and configure the following components.

Option	Description
Load Balancing	Specify how to choose an uplink. • **Inherit from vSwitch**. Choose the uplink that is selected for the associated virtual switch. • **Route based on IP hash**. Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash. • **Route based on source MAC hash**. Choose an uplink based on a hash of the source Ethernet. • **Route based on originating port ID**. Choose an uplink based on the originating port ID. • **Use explicit failover order**. Always use the highest order uplink from the list of active adapters which passes failover detection criteria . **Note:** IP-based teaming requires the physical switch to be configured with EtherChannel. For all other options, EtherChannel must be disabled.
Network Failover Detection	Specify the method to use for failover detection. • • **Inherit from vSwitch**. Inherits the respective configuration of the associated virtual switch. • **Link Status only**. Relies only on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by a spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch. • **Beacon only**. Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine a link failure. This detects many of the failures that are not detected by link status only. **Note:** Do not use beacon probing with IP-hash load balancing.
Notify Switches	Select **Yes**, **No**, or **Inherit from vSwitch** to notify switches if a failover occurs.

Option	Description
	If you select **Yes**, when a virtual NIC is connected to the distributed switch or that virtual NIC's traffic is routed over a different physical NIC in the team because of a failover event, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this process is preferred for the lowest latency of failover occurrences and migrations with vMotion. **Note:** Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode.
Failback	Select **Yes**, **No**, or **Inherit from vSwitch** to disable or enable failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. If failback is set to the default setting of **Yes**, the adapter returns to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. If failback is set to **No**, a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
Failover Order	Specify how to distribute the workload for uplinks. If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, set this condition by moving them into different groups: • **Active Uplinks**. Continue to use the uplink when the network adapter connectivity is up and active. • **Standby Uplinks** . Use this uplink if one of the active adapter's connectivities is down. **Note:** When using IP-hash load balancing, do not configure standby uplinks. You cannot configure failover order if any of the port group components are configured to inherit the configuration from the associated virtual switch.

8. Optional: To configure traffic shaping, expand **Traffic shaping**, click **Enabled**, and specify the following parameters.

Option	Description
Average Bandwidth	Establishes the number of bits per second to limit across a port, averaged over time—the allowed average load.
Peak Bandwidth	The maximum number of bits per second to limit across a port when it is sending/receiving a burst of traffic. This is the maximum bandwidth used by a port whenever it is using its burst bonus.
Burst Size	The maximum number of bytes to limit in a burst. If this parameter is set, a port might gain a burst bonus when it does not use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by **Average Bandwidth**, it might be allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter represents the

Option	Description
	maximum number of bytes that might be accumulated in the burst bonus and so transferred at a higher speed.

Traffic shaping policy is applied to the traffic of each virtual network adapter attached to the virtual switch.

9. Click **Save** to apply your changes.

Remove a Virtual Switch Port Group in the VMware Host Client

You can remove port groups from virtual switches in case you no longer need the associated labeled networks.

Verify that there are no VMkernel NICs and no powered-on virtual machines connected to the port group that you want to remove.

1. Click **Networking** in the VMware Host Client inventory and click the **Port groups** tab.
2. Right-click the port group that you want to remove and select **Remove** from the pop-up menu.
3. To remove the port group, click **Remove**.
4. Optional: Click **Refresh** to verify that you have removed the port group.

Managing Virtual Switches in the VMware Host Client

In the VMware Host Client, you can configure various virtual switch settings, such as link discovery, NIC teaming, and traffic shaping.

View Virtual Switch Information in the VMware Host Client

In the VMware Host Client, you can view information about virtual switches, such as configuration, network details, virtual switch topology, and so on.

1. Click **Networking** in the VMware Host Client inventory and click **Virtual switches**.
2. Click on a switch from the list of available virtual switches.

   Information about virtual switch configuration, network details, and virtual switch topology is displayed.

Add a Standard Virtual Switch in theVMware Host Client

In theVMware Host Client, you can add a standard virtual switch to provide network connectivity for the host that you are managing and for the virtual machines on that host, and to handle VMkernel traffic. Depending on the type of connection that you want to create, you can create vSphere standard switch with a VMkernel adapter, connect an existing physical network adapter to the new switch, or create the switch with a virtual machine port group.

1. Right-click **Networking** in theVMware Host Client inventory and click **Add standard vSwitch** in the pop-up menu.
2. Optional: Click **Add uplink** to add a new physical uplink to a virtual switch.
3. Enter a name for the virtual switch and click **Create virtual switch**.
4. Select an uplink for the virtual switch.
5. Expand **Link discovery** and select an option for the virtual switch mode.

Operation	Description
Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere Standard Switch is not available to the switch administrator.

Operation	Description
Advertise	ESXi makes information about the vSphere Standard Switch available to the switch administrator, but does not detect and display information about the physical switch.
Both	ESXi detects and displays information about the associated physical switch and makes information about the vSphere Standard Switch available to the switch administrator.
None	ESXi does not detect or display information about the associated physical switch port, and information about the vSphere Standard Switch is not available to the switch administrator.

6. In the Protocol section, select **Cisco Discovery Protocol** from the drop-down menu.
7. Expand **Security** and accept or reject promiscuous mode, MAC address changes, and forged transmits of the virtual machines attached to the standard switch.

Option	Description
Promiscuous mode	• **Reject**. The VM network adapter receives only frames that are addressed to the virtual machine. • **Accept**.The virtual switch forwards all frames to the virtual machine in compliance with the active VLAN policy for the port to which the VM network adapter is connected. **Note:** Promiscuous mode is insecure mode of operation. Firewalls, port scanners, intrusion detection systems, must run in promiscuous mode.
MAC address changes	• **Reject**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter (set in the `.vmx` configuration file), the switch drops all inbound frames to the adapter. If the guest OS changes the effective MAC address of the virtual machine back to the MAC address of the VM network adapter, the virtual machine receives frames again. • **Accept**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter, the switch allows frames to the new address to pass.
Forged transmits	• **Reject**. The switch drops any outbound frame from a virtual machine adapter with a source MAC address that is different from the one in the `.vmx` configuration file. • **Accept**. The switch does not perform filtering, and permits all outbound frames.

8. Click **Add**.

Remove a Standard Virtual Switch in the VMware Host Client

You can remove the virtual standard switch if you no longer need it.

1. Click **Networking** in the VMware Host Client inventory and click the **Virtual switches** tab.
2. Right-click the virtual switch that you want to remove from the list and click **Remove**.
3. Click **Yes**.

Add a Physical Uplink to a Virtual Switch in the VMware Host Client

You can connect multiple adapters to a single vSphere standard switch to provide NIC teaming. The team can share traffic and provide failover.

1. Click **Networking** in the VMware Host Client inventory and click **Virtual switches**.
2. Click a virtual switch from the list and click **Add uplink**.
3. Select a physical NIC from the available options.
4. Click **Save**.

Edit Virtual Switch Settings in theVMware Host Client

In theVMware Host Client, you can edit virtual switch settings, such as the virtual switch uplinks.

1. Click **Networking** in theVMware Host Client inventory and click **Virtual switches**.
2. Right-click the virtual switch that you want to edit and click **Edit Settings**.
3. Optional: Click **Add uplink** to add a new physical uplink to the virtual switch.
4. Change the maximum transmission unit (MTU).

   The MTU improves the networking efficiency by increasing the amount of payload data transmitted with a single packet, that is, enabling jumbo frames.
5. Optional: Click the **Remove** icon (⊗) to remove the old uplink from the virtual switch.
6. Expand **Link discovery** and select an option for the virtual switch mode.

Operation	Description
Listen	ESXi detects and displays information about the associated physical switch port, but information about the vSphere Standard Switch is not available to the switch administrator.
Advertise	ESXi makes information about the vSphere Standard Switch available to the switch administrator, but does not detect and display information about the physical switch.
Both	ESXi detects and displays information about the associated physical switch and makes information about the vSphere Standard Switch available to the switch administrator.
None	ESXi does not detect or display information about the associated physical switch port, and information about the vSphere Standard Switch is not available to the switch administrator.

7. In the Protocol section, select **Cisco Discovery Protocol** from the drop-down menu.
8. Expand **Security** and accept or reject promiscuous mode, MAC address changes, and forged transmits of the virtual machines attached to the standard switch.

Option	Description
Promiscuous mode	• **Reject**. The VM network adapter receives only frames that are addressed to the virtual machine. • **Accept**.The virtual switch forwards all frames to the virtual machine in compliance with the active VLAN policy for the port to which the VM network adapter is connected. **Note:** Promiscuous mode is insecure mode of operation. Firewalls, port scanners, intrusion detection systems, must run in promiscuous mode.
MAC address changes	• **Reject**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter (set in the `.vmx` configuration file), the switch drops all inbound frames to the adapter. If the guest OS changes the effective MAC address of the virtual machine back to the MAC address of the VM network adapter, the virtual machine receives frames again. • **Accept**. If the guest OS changes the effective MAC address of the virtual machine to a value that is different from the MAC address of the VM network adapter, the switch allows frames to the new address to pass.
Forged transmits	• **Reject**. The switch drops any outbound frame from a virtual machine adapter with a source MAC address that is different from the one in the `.vmx` configuration file. • **Accept**. The switch does not perform filtering, and permits all outbound frames.

9. Optional: Expand **NIC teaming** and configure the following components.

Option	Description
Load Balancing	Specify how to choose an uplink. • **Route based on IP hash**. Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash. • **Route based on source MAC hash**. Choose an uplink based on a hash of the source Ethernet. • **Route based on originating port ID**. Choose an uplink based on the originating port ID. • **Use explicit failover order**. Always use the highest order uplink from the list of Active adapters which passes failover detection criteria. **Note:** IP-based teaming requires the physical switch to be configured with EtherChannel. For all other options, EtherChannel must be disabled.
Network Failover Detection	Specify the method to use for failover detection. • **Link Status only**. Relies only on the link status that the network adapter provides. This option detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being

Option	Description
	blocked by spanning tree or that is misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch. • **Beacon only**. Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. This detects many of the failures previously mentioned that are not detected by link status alone. **Note:** Do not use beacon probing with IP-hash load balancing.
Notify Switches	Select **Yes**, **No**, or **Inherit from vSwitch** to notify switches in the case of failover. If you select **Yes**, whenever a virtual NIC is connected to the distributed switch or whenever that virtual NIC's traffic might be routed over a different physical NIC in the team because of a failover event, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this process is desirable for the lowest latency of failover occurrences and migrations with vMotion. **Note:** Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode.
Failback	Select **Yes**, **No**, or **Inherit from vSwitch** to disable or enable failback. This option determines how a physical adapter is returned to active duty after recovering from a failure. If failback is set to **Yes** (default), the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any. If failback is set to **No**, a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
Failover Order	Specify how to distribute the work load for uplinks. If you want to use some uplinks but reserve others for emergencies in case the uplinks in use fail, set this condition by moving them into different groups: • **Active Uplinks**. Continue to use the uplink when the network adapter connectivity is up and active. • **Standby Uplinks** . Use this uplink if one of the active adapter's connectivities is down. **Note:** When using IP-hash load balancing, do not configure standby uplinks.

10. Optional: To configure traffic shaping, expand **Traffic shaping**, click **Enabled**, and specify the following parameters.

Option	Description
Average Bandwidth	Establishes the number of bits per second to allow across a port, averaged over time—the allowed average load.
Peak Bandwidth	The maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This tops the bandwidth used by a port whenever it is using its burst bonus.

Option	Description
Burst Size	The maximum number of bytes to allow in a burst. If this parameter is set, a port may gain a burst bonus when it doesn't use all its allocated bandwidth. Whenever the port needs more bandwidth than specified by **Average Bandwidth**, it may be allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter tops the number of bytes that may be accumulated in the burst bonus and then transferred at a higher speed.

Traffic shaping policy is applied to the traffic of each virtual network adapter attached to the virtual switch.

11. Click **Save**.

Managing Physical Network Adapters in the VMware Host Client

Assign a physical adapter to a standard switch to provide connectivity to virtual machines and VMkernel adapters on the host that you are managing.

View Physical Network Adapter Information in the VMware Host Client

In the VMware Host Client, you can view various information about physical network adapter (NIC) configuration and settings.

1. Click **Networking** in the VMware Host Client inventory and click **Physical NICs**.
2. Click on the network adapter that you want to view information about.

Edit Physical NICs in the VMware Host Client

You can edit physical NIC speed by using the VMware Host Client.

1. Click **Networking** in the VMware Host Client inventory and click **Physical NICs**.
2. Select the NIC in the table that you want to edit.
3. Click **Edit settings** and select a speed from the drop-down menu.
4. Click **Save**.

Managing VMkernel Network Adapters in the VMware Host Client

In the VMware Host Client, you can add and remove VMkernel network adapters (NICs), as well as view and modify the VMkernel NIC settings.

View VMkernel Network Adapter Information in the VMware Host Client

In the VMware Host Client, you can view information about VMkernel network adapters (NICs), such as TCP/IP configuration, network details, virtual switch topology, and so on.

1. Click **Networking** in the VMware Host Client inventory and click **VMkernel NICs**.
2. Click a NIC in the list to display configuration and topology details.

Add a VMkernel Network Adapter in theVMware Host Client

You can add a VMkernel network adapter (NIC) on a VMware vSphere® Standard Edition™ switch to provide network connectivity for hosts. The VMkernel NIC also handles the system traffic for VMware vSphere® vMotion®, IP storage, Fault Tolerance, logging,vSAN, and so on.

1. Right-click **Networking** in theVMware Host Client inventory and click **Add VMkernel NIC**.
2. In the **Add VMkernel NIC** dialog box, configure the settings for the VMkernel adapter.

Option	Description
New port group Label	Adding a VMkernel NIC also adds a port group. Specify a name for that port group.
VLAN ID	Enter a VLAN ID to determine the VLAN for the network traffic of the VMkernel adapter to use.
IP Version	Select IPv4, IPv6, or both. **Note:** The IPv6 option does not appear on hosts that do not have IPv6 enabled.

3. Select a virtual switch from the drop-down menu.
4. Optional: Expand the IPv4 settings section to select an option for obtaining IP addresses.

Option	Description
Use DHCP to obtain IP settings	IP settings are obtained automatically. A DHCP server must be present on the network.
Use static IP settings	Enter the IPv4 address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack.

5. Optional: Expand the IPv6 settings section to select an option for obtaining IPv6 addresses.

Option	Description
DHCPv6	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Auto Configuration	Use router advertisement to obtain IPv6 addresses.
Static IPv6 Addresses	1. Click **Add address** to add a new IPv6 address. 2. Enter the IPv6 address and subnet prefix length.

6. Select a TCP/IP stack from the drop-down menu.

   After you set a TCP/IP stack for the VMkernel adapter, you cannot change it. If you select the vMotion or the Provisioning TCP/IP stack, you can use only this stack to handle vMotion or for Provisioning traffic on the host. All VMkernel adapters for vMotion on the default TCP/IP stack are disabled for future vMotion sessions. If you use the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are disabled, and you cannot perform some operations. Such operations include traffic Provisioning, such as virtual machine cold migration, cloning, and snapshot migration.

7. Optional: Select the services to enable for the default TCP/IP stack on the host.

   vMotion enables the VMkernel adapter to advertise itself to another host as the network connection where vMotion traffic is sent. You cannot use vMotion to perform migrations to selected hosts if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or if no adapters use the vMotion TCP/IP stack.

8. Review your setting selections and click **Create**.

Edit VMkernel Network Adapter Settings in theVMware Host Client

You might have to change the supported traffic type for a VMkernel network adapter, or the way IPv4 or IPv6 addresses are obtained.

1. Click **Networking** in theVMware Host Client inventory and click **VMkernel NICs**.
2. Select the VMkernel adapter that resides on the target standard switch, click **Actions**, and select **Edit settings** from the drop-down menu.
3. Optional: Edit the VLAN ID.

   The VLAN ID determines the VLAN that the network traffic of the VMkernel adapter uses.

4. Optional: To edit the IP version, select IPv4, IPv6, or both from the drop-down menu.

   Note: The IPv6 option does not appear on hosts that do not have IPv6 enabled.

5. Optional: Expand the IPv4 settings section to select an option for obtaining IP addresses.

Option	Description
Use DHCP to obtain IP settings	IP settings are obtained automatically. A DHCP server must be present on the network.
Use static IP settings	Enter the IPv4 address and subnet mask for the VMkernel adapter. The VMkernel Default Gateway and DNS server addresses for IPv4 are obtained from the selected TCP/IP stack.

6. Optional: Expand the IPv6 settings section to select an option for obtaining IPv6 addresses.

Option	Description
DHCPv6	Use DHCP to obtain IPv6 addresses. A DHCPv6 server must be present on the network.
Auto Configuration	Use a router advertisement to obtain IPv6 addresses.
Static IPv6 Addresses	1. Click **Add address** to add an IPv6 address. 2. Enter the IPv6 address and subnet prefix length.

7. Optional: Select the service to enable or disable for the default TCP/IP stack on the host.

   vMotion enables the VMkernel adapter to advertise itself to another host as the network connection where the vMotion traffic is sent. It is not possible to use vMotion to perform migrations to selected hosts if the vMotion service is not enabled for any VMkernel adapter on the default TCP/IP stack, or if no adapters use the vMotion TCP/IP stack.

8. Review your setting modifications and click **Save** to apply your changes.

Remove a VMkernel Network Adapter in the VMware Host Client

In the VMware Host Client, you can remove a VMkernel network adapter if you no longer need it.

1. Click **Networking** in the VMware Host Client inventory and click **VMkernel NICs**.
2. Right-click the VMkernel adapter that you want to remove and click **Remove**.
3. Click **Confirm** to remove the network adapter.

View TCP/IP Stack Configuration on a Host in the VMware Host Client

You can view the DNS and routing configuration of a TCP/IP stack on a host. You can also view the IPv4 and IPv6 routing tables, the congestion control algorithm, and the maximum number of allowed connections.

1. Click **Networking** in the host inventory and click **TCP/IP stacks**.
2. Click a stack from the list.
   The configuration settings of the stack you selected are displayed.

Change the Configuration of a TCP/IP Stack on a Host in theVMware Host Client

You can change the DNS and default gateway configuration of a TCP/IP stack on a host. You can also change the congestion control algorithm, the maximum number of connections, and the name of custom TCP/IP stacks.

1. Click **Networking** in theVMware Host Client inventory and click **TCP/IP stacks**.
2. Right-click a stack from the list and select **Edit settings**.
   The Edit TCP/IP configuration - Provisioning stack dialog box opens.
3. Specify how the host obtains settings for this TCP/IP stack.
   - Select the **Use DHCP services from the following adapter** radio button, and select an adapter from which to receive the default settings configuration for the TCP/IP stack.
   - Select the **Manually configure the settings for this TCP/IP stack** to change the settings configuration.

Option	Description	
Basic configuration	**Host name**	Edit the name of your local host.
	Domain name	Edit the domain name.
	Primary DNS server	Enter a preferred DNS server IP address.
	Secondary DNS server	Type an alternate DNS server IP address.
	Search domains	Specify DNS suffixes to use in DNS search when resolving unqualified domain names.
Routing	Edit the IPv4 and IPv6 gateway information. **Note:** Removing the default gateway might cause you to lose your connection to the host.	
Advanced Settings	Edit the congestion control algorithm and the maximum number of connections.	

4. Click **Save**.

Configuring ESXi Firewall in the VMware Host Client

ESXi includes a firewall that is enabled by default. At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the host security profile.

As you open ports on the firewall, consider that unrestricted access to services running on an ESXi host may expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to allow access only from authorized networks.

Note: The firewall also allows Internet Control Message Protocol, or ICMP, pings and communication with DHCP and DNS (UDP only) clients.

Manage ESXi Firewall Settings by Using the VMware Host Client

When you are logged in to an ESXi host with the VMware Host Client, you can configure incoming and outgoing firewall connections for a service or a management agent.

Note: If different services have overlapping port rules, enabling one service might implicitly enable other services. You can specify which IP addresses are allowed to access each service on the host to avoid this problem.

1. Click **Networking** in the inventory.
2. Click **Firewall rules**.

   The VMware Host Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.
3. For some services you can manage service details. Right-click a service and select an option from the pop-up menu.
   - Use the Start, Stop, or Restart buttons to change the status of a service temporarily.
   - Change the Startup Policy to configure the service to start and stop with the host, the firewall ports, or manually.

Add Allowed IP Addresses for an ESXi Host by Using the VMware Host Client

By default, the firewall for each service allows access to all IP addresses. To restrict traffic, configure each service to allow traffic only from your management subnet. You can also deselect some services if your environment does not use them.

1. Click **Networking** in the inventory and click **Firewall rules**.
2. Click a service from the list and click **Edit settings**.
3. In the Allowed IP Addresses section, click **Only allow connections from the following networks** and enter the IP addresses of networks that you want to connect to the host.
   Separate IP addresses with commas. You can use the following address formats:
   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64
4. Click **OK**.

Monitoring Networking Events and Tasks in the VMware Host Client

You can view details about the events and tasks associated with the port groups, virtual switches, physical network adapters, VMkernel network adapters, and TCP/IP stacks on the ESXi host that you are managing.

Monitor Port Groups in the VMware Host Client

In the VMware Host Client, you can monitor port group performance by viewing the events and tasks of the port groups on the host.

1. Click **Networking** in the inventory.
2. Click **Port groups**.
3. Click a port group from the list.
   The port group expands in the VMware Host Client inventory.
4. Click **Monitor** under the port group name in the VMware Host Client inventory.
5. Optional: Click **Events** to view the events associated with the port group.

Monitor Virtual Switches in the VMware Host Client

In the VMware Host Client, you can monitor virtual switch performance by viewing the events and tasks of the virtual switches on the host.

1. Click **Networking** in the inventory.
2. Click **Virtual switches**.
3. Click a virtual switch from the list.
   The virtual switch expands in the VMware Host Client inventory.
4. Click **Monitor** under the virtual switch name in the VMware Host Client inventory.
5. Optional: Click **Events** to view the events associated with the virtual switch.

Monitor Physical Network Adapters in the VMware Host Client

In the VMware Host Client, you can monitor physical network adapter (NIC) performance by viewing the events and tasks of the physical NICs on the host.

1. Click **Networking** in the inventory.
2. Click **Physical NICs**.
3. Click a physical network adapter from the list.
   The physical network adapter expands in the VMware Host Client inventory.
4. Click **Monitor** under the physical network adapter name in the VMware Host Client inventory.
5. Optional: Click **Events** to view the events associated with the physical network adapter.

Monitor VMkernel Network Adapters in the VMware Host Client

In the VMware Host Client, you can monitor VMkernel network adapter performance by viewing the events and tasks of the VMkernel network adapters on the host.

1. Click **Networking** in the inventory.
2. Click **VMkernel NICs**.
3. Click a VMkernel network adapter from the list.
   The VMkernel network adapter expands in the VMware Host Client inventory.

4. Click **Monitor** under the VMkernel network adapter name in the VMware Host Client inventory.
5. Optional: Click **Events** to view the events associated with the VMkernel network adapter.

Monitor TCP/IP Stacks in the VMware Host Client

In the VMware Host Client, you can monitor TCP/IP stacks performance by viewing the events and tasks of the TCP/IP stacks on the host.

1. Click **Networking** in the inventory.
2. Click **TCP/IP stacks**.
3. Click a TCP/IP stack from the list.
   The TCP/IP stack expands in the VMware Host Client inventory.
4. Click **Monitor** under the TCP/IP stack name in the VMware Host Client inventory.
5. Optional: Click **Events** to view the events associated with the TCP/IP stack.
6. Optional: Click **Tasks** to view the tasks associated with the TCP/IP stack.

Setup for Windows Server Failover Clustering on VMware vSphere

Setup for Windows Server Failover Clustering describes the supported configurations for a WSFC with shared disk resources you can implement using virtual machines with Failover Clustering for Windows Server 2012 and above releases. You get step-by-step instructions for each configuration and a checklist of clustering requirements and recommendations.

Unless stated otherwise, the term Windows Server Failover Clustering (WSFC) applies to Failover Clustering with Windows Server 2012 and above releases.

Setup for Windows Server Failover Clustering covers ESXi and VMware® vCenter® Server.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

This information is for system administrators who are familiar with VMware technology and Failover Clustering for Windows.

Note: This is not a guide to using Failover Clustering for Windows. Use your Microsoft documentation for information about installation and configuration of Microsoft Cluster Service or Failover Clustering.

Note:

All instances of "WSFC" in this document and elsewhere is intended to refer to all Windows OS and Microsoft application clustering configurations which utilize one or more shared disks among the clustered nodes, namely:

- The Microsoft Cluster Service (MSCS)
- The Windows Server Failover Clustering (WSFC)
- Microsoft SQL Server Always On Failover Cluster Instances (FCI)

Note: Other WSFC-based solutions not accessing shared storage such as SQL Server Always On Availability Groups or Exchange Database Availability Group, require no special storage configurations on the vSphere side using VMFS or NFS. This guide should not be used for such configurations.

Getting Started with WSFC on VMware®vSphere®

VMware® vSphere® supports Windows clustering using WSFC across virtual machines. Clustering virtual machines can reduce the hardware costs of traditional high-availability Windows clusters.

Note: vSphere High Availability (vSphere HA) supports a Windows clustering solution. *vSphere Availability* describes vSphere HA functionality.

Clustering Configuration Overview

Several applications use clustering, including stateless applications such as Web servers, and applications with built-in recovery features such as database servers. You can set up WSFC clusters in several configurations, depending on your environment.

A typical clustering setup includes:

- Disks resources that are shared between nodes. A shared disk is required as a quorum disk. In a cluster of virtual machines across physical hosts, shared disks can be RDMs, vVol or VMFS VMDKs. If you are using RDMs or vVol as shared disks, they can accessed using Fibre Channel (FC) SAN, FCoE or iSCSI. If you are using VMFS VMDKs as

shared disks, only FC SAN connected storage devices are supported. A WSFC must have a homogenous set of disks. This means that if the configuration is done with disks attached using FC SAN, then all of the cluster disks should be FC SAN only. Mixed mode is not supported.

In ESXi 7.0, clustered VMDKs on VMFS datastores are supported in configurations when the VMs hosting the nodes of a cluster are located on different ESXi hosts, known as cluster-across-boxes (CAB) configuration.

Note: **VMDKs** in this guide refers to Shared disk files from VMFS datastore shared in physical compatibility mode (Attached to SCSI controller with bus sharing mode set to **Physical**) for cluster across physical machines. This is also known as Clustered VMDKs.

Hosting virtual nodes of a WSFC on a Single Host

A cluster of WSFC virtual machines on a single host (also known as a cluster in a box or CIB) consists of clustered virtual machines on the same ESXi host. The virtual machines are connected to the same storage, either local or remote. This configuration protects against failures at the operating system and application level, but it does not protect against hardware failures.

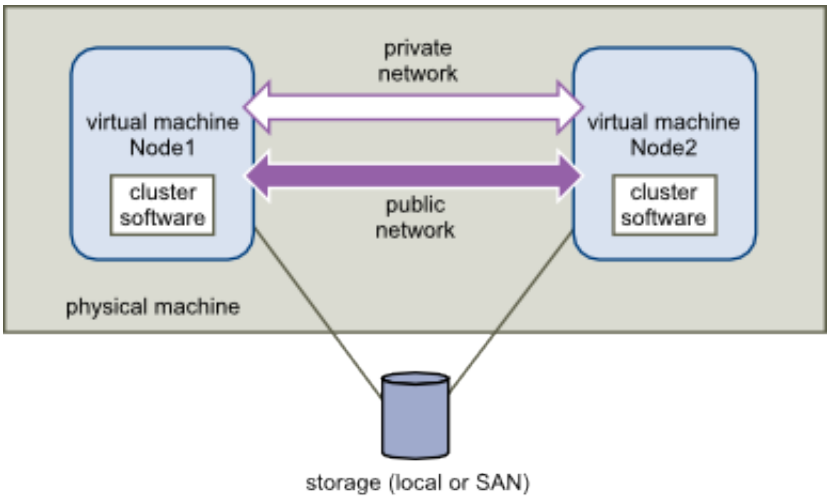
Note: Do not host virtual nodes of a WSFC on the same ESXi host for a production deployment.

Note: Windows Server 2012 and above releases support up to five nodes (virtual machines).

The following figure shows a cluster in a box setup.

- Two virtual machines on the same ESXi host run WSFC.
- The virtual machines share a private network connection for the private heartbeat and a public network connection.
- Each virtual machine is connected to shared storage, which can be local or on a SAN.
- Each shared disk should be attached to SCSI controller with bus sharing mode set to **Virtual**.

Figure 112: Virtual Machines Clustered on a Single Host



Clustering Virtual Machines Across Physical Hosts

A cluster of virtual machines across physical ESXi hosts (also known as a cluster across boxes or CAB) protects against software failures and hardware failures on the physical ESXi hosts by placing the cluster nodes on separate ESXi hosts. This configuration requires shared storage for the clustered disk resources.

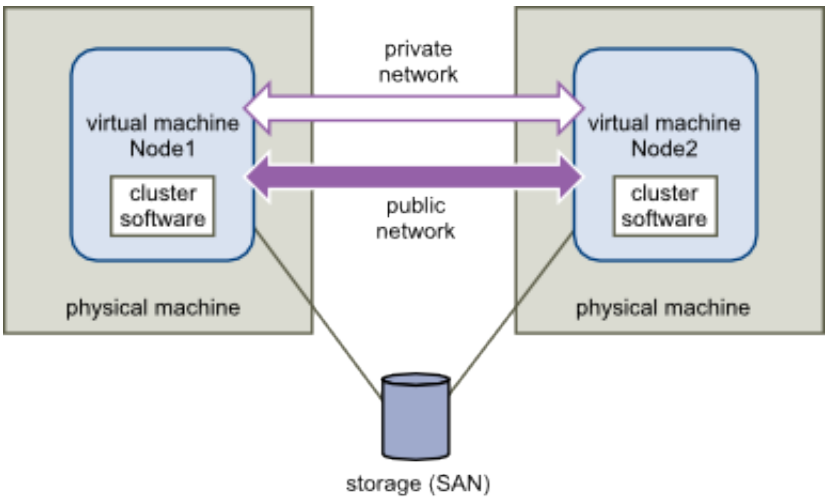
The following figure shows a cluster-across-boxes setup.

- Two virtual machines on two different ESXi hosts run WSFC.

- The virtual machines share a private network connection for the private heartbeat and a public network connection.
- Each virtual machine is connected to shared storage.

Note: In a cluster of virtual machines across physical hosts, shared disks can be physical mode or vVol with vSphere 6.7 or later. You can use VMFS VMDKs with vSphere 7.0 or later. If you are using RDMs or vVol as shared disks, they can be on Fibre Channel (FC) SAN, FCoE or iSCSI. If you are using VMFS VMDKs as shared disks, they must be on FC SAN only. A clustered disk must have a homogenous set of disks. This means that if the configuration is done with FC SAN, then all of the cluster disks should be FC SAN only. Mixed mode is not supported.

Figure 113: Virtual Machines Clustered Across Hosts



Note: Windows Server 2012 and above systems support up to five nodes (virtual machines). For supported guest operating systems see Table 4.

Note: Private and Public network interconnect can share a single virtual NIC in a VM.

You can expand the cluster-across-boxes model and place multiple virtual machines on multiple ESXi hosts. For example, you can consolidate three clusters of two physical machines each to two ESXi hosts with four virtual machines each.

Clustering Physical Machines with Virtual Machines

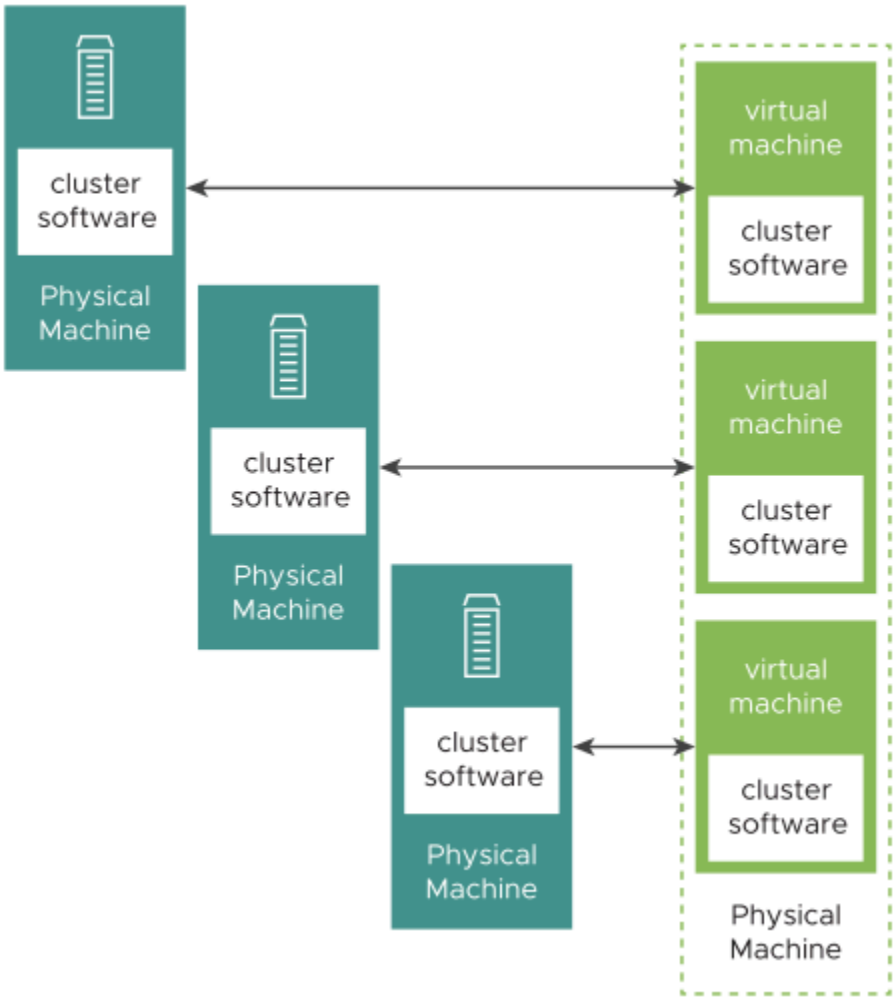
For a simple WSFC clustering solution with low hardware requirements with RDMs, you might choose to have one standby host.

Set up your system to have a virtual machine corresponding to each physical machine on the standby host, and create clusters, one each for each physical machine and its corresponding virtual machine. In case of hardware failure in one of the physical machines, the virtual machine on the standby host can take over for that physical host.

The following figure shows a standby host using three virtual machines on a single ESXi host. Each virtual machine is running WSFC.

Note: This solution is not applicable for vVol and clustered VMDKs.

Figure 114: Clustering Physical and Virtual Machines



Hardware and Software Requirements for WSFC on vSphere

All vSphere WSFC configurations require certain hardware and software components.

The following table lists hardware and software requirements that apply to all vSphere WSFC configurations.

Table 530: Clustering Requirements

Component	Requirement
Virtual SCSI adapter	LSI Logic SAS for Windows Server 2012 and above. VMware Paravirtual for Windows Server 2012 and above. (recommended)
Operating system	Windows Server 2012 and above releases. For supported guest operating systems see Table 4.
Virtual NIC	VMXNET3 is required. You must activate in-guest Windows Receive Side Scaling (RSS) on the virtual NIC. **Note:** Drivers, improvements and updates to the VMXNET3 virtual NIC are delivered through VMware Tools. Upgrade to the latest version of VMware Tools on any VM using the VMXNET3 virtual NIC.

Component	Requirement
I/O timeout	Set to 60 seconds or more. Modify `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue`. The system might reset this I/O timeout value if you re-create a cluster. You must reset the value in that case.
Disk format	pRDM (physical compatibility mode) vVol disks can be thin or thick format VMFS VMDKs with vSphere 7.0 `eagerzeroedthick` format
Disk and networking setup	Add networking before disks.
Number of nodes	Windows Server 2012 and above: up to five-node clustering For supported guest operating systems see Table 4.
NTP server	Synchronize Windows Active Directory domain controllers and WSFC nodes with a common NTP server, and deactivate host-based time synchronization. See KB 1189 for more information.

The following table lists requirements that apply to Clustered VMDK as a disk resource for a WSFC.

Table 531: Additional Requirements for Clustered VMDK WSFC

Component	Requirement
Windows Cluster Parameters	Set the Windows Cluster Parameter QuorumArbitrationTimeMax to 60
Physical disk /Storage Array LUN	• The physical disk that virtual disks are stored on must support ATS SCSI • The physical disk must also support SCSI-3 Persistent Reservations, specifically Write Exclusive All Registrants (WEAR) type reservations
VMFS Datastore	• VMFS version must be VMFS6 • Fibre Channel (FC) only • The datastore must have attribute **ClusteredVMDK** set. See Activating Clustered VMDK Support.

Supported Shared Storage Configurations

Different WSFC cluster setups support different types of shared storage configurations. Some setups support more than one type. Select the recommended type of shared storage for best results.

Differences between Physical compatibility RDMs and Virtual compatibility RDMs

An RDM (Raw Device Mapped) is a special mapping file in a VMFS volume that manages metadata for its mapped device. The mapping file is presented to the management software as an ordinary disk file, available for file-system operations. To the virtual machine, the storage virtualization layer presents the mapped device as a virtual SCSI device. There are two types of compatibility modes for RDMs.

- A Physical compatibility RDM (pRDM), specifies minimal SCSI virtualization of the mapped device.
  - Virtual Machine Snapshots are not available when the RDM is used in physical compatibility mode.
  - RDMs in physical compatibility mode are required to allow SCSI commands be directly passed to a LUN to satisfy the requirements of SCSI-3 Persistent Reservations used by WSFC.

- A Virtual compatibility RDM (vRDM), specifies full virtualization of the mapped device.
  - VMkernel sends only READ and WRITE to the mapped device. The mapped device appears to the guest operating system the same as a virtual disk file in a VMFS volume.
  - If you are using a raw disk in virtual mode, you can realize the benefits of VMFS, such as advanced file locking for data protection and snapshots for streamlining development processes.
  - Virtual mode is more portable across storage hardware than physical mode, presenting the same behavior as a virtual disk file.
  - Supported for CIB configuration only.
    Note: Do not use cluster-in-a-box configuration for a production deployment.

For more information, see KB 2147661.

Table 532: Shared Storage Requirements

Storage Type	Clusters on One Physical Machine (Cluster in a Box)	Clusters Across Physical Machines (Cluster Across Boxes)	Clusters of Physical and Virtual Machines (Standby Host Clustering)
Clustered VMDK	No	Yes	No
VMDK in Virtual compatibility mode (SCSi controller sharing mode set to virtual)	Yes	No	No
pRDM (physical compatibility mode)	No	Yes (recommended)	Yes
vRDM (virtual compatibility mode)	Yes (not recommended)	No	No

Note: The multi-writer feature must not be used for a clustered disk resource for WSFC.

Use of in guest options for storage such as iSCSI or SMB shares within guest operating systems configured with WSFC, in any configuration supported by Microsoft, is transparent to ESXi hosts and there is no need for explicit support statements from VMware.

Round Robin Path Selection Policy (PSP_RR) Support for disk resources used by WSFC

ESXi 7.0 supports PSP_RR for WSFC.

- ESXi 7.0 supports PSP_RR for Windows Server 2012 and above releases. Windows Server 2008 SP2 and earlier are not supported.
- PSPs configured in mixed mode is supported. In a 2 node WSFC cluster in CAB configuration one ESXi host can be configured to use PSP_FIXED and the other ESXi host can use PSP_RR.
- All hosts must be running ESXi 6.0 or later.
- Mixed mode configurations of ESXi 6.0 or later with previous ESXi releases are not supported.

iSCSI Support for WSFC

ESXi 7.0 supports iSCSI storage and up to 5 node WSFC clusters.

- ESXi 7.0 supports iSCSI for Windows Server 2012 and above releases. Windows Server 2008 SP2 and earlier are not supported.

- Cluster-across-box (CAB) and cluster-in-a-box (CIB) are supported. A mixture of CAB and CIB is not supported.
- Clustered VMDKs on VMFS datastore in CAB are not supported over iSCSI.
- No qualification is needed for software iSCSI initiator in a guest operating system.
- N+1 cluster configuration comprising of a cluster between "N" virtual machines on separate ESXi hosts and one physical machine running Windows natively is supported.
- All hosts must be running ESXi 6.0 or later.
- Mixed cluster nodes running FC or FCOE and iSCSI are not supported. Mixed mode refers to shared disks (for the same Windows Failover cluster) from different kinds of storage such as FC, iSCSI, FCoE or the shared disk type being different such as RDM, VMDK or VVOls.
- Cluster nodes registered to hosts with different ESXi versions are not supported.
- Mixed mode of iSCSI config is supported.

FCoE Support for WSFC

ESXi 7.0 supports FCoE storage and up to 5 node WSFC clusters.

- ESXi 7.0 supports FCoE for Windows Server 2012 and above releases. Windows Server 2008 SP2 and earlier are not supported.
- Cluster-across-box (CAB) and cluster-in-a-box (CIB) are supported. A mixture of CAB and CIB is not supported.
- CAB configurations are supported with some cluster nodes on physical hosts. In a CAB configuration, a max of one virtual machine in a host can see a LUN.
- Clustered VMDK is not supported on a datastore connected over FCoE.
- N+1 cluster configuration, in which one ESXi host has virtual machines which are secondary nodes and one primary node is a physical box are supported.
- Required DRS affinity (CIB) or Anti-affinity (CAB) rules for WSFC virtual machines.
- All hosts must be running FCoE initiators. Mixed cluster nodes running FC and FCoE are not supported.
- Mixed mode FCoE configuration is supported.

vMotion support for WSFC

vSphere 7.0 supports vMotion of a VM hosting a node of a WSFC.

Pre-requisites for vMotion support:

- vMotion is supported only for a cluster of virtual machines across physical hosts (CAB).
- The vMotion network must be a 10Gbps Ethernet link. 1Gbps Ethernet link for vMotion of WSFC virtual machines is not supported.
- vMotion is supported for Windows Server 2012 and above releases. Windows Server 2008 SP2 and earlier are not supported.
- The WSFC cluster heartbeat time-out must be modified at least to the values listed below:
  - `(get-cluster -name <cluster-name>).SameSubnetThreshold = 10`
  - `(get-cluster -name <cluster-name>).CrossSubnetThreshold = 20`
  - `(get-cluster -name <cluster-name>).RouteHistoryLength = 40`
- The virtual hardware version for the WSFC virtual machine must be version 11 and later.

Modifying the WSFC heartbeat time-out:

WSFC nodes use the network to send heartbeat packets to other nodes of the cluster. If a node does not receive a response from another node for a specified period of time, the cluster removes the node from cluster membership. By default, a guest cluster node is considered down if it does not respond within 5 seconds in Windows 2012, 2012 R2. Other nodes that are members of the cluster will take over any clustered roles that were running on the removed node.

An WSFC virtual machine can stall for a few seconds during vMotion. If the stall time exceeds the heartbeat time-out interval, then the guest cluster considers the node down and this can lead to unnecessary failover. To allow leeway and make the guest cluster more tolerant, the heartbeat time-out interval needs to be modified to allow at least 10 missed heartbeats. The property that controls the number of allowed heart misses is **SameSubnetThreshold**. You will need to modify this from its default value to at least 10. From any one of the participating WSFC cluster nodes run the following command:

```
(get-cluster -name <cluster-name>).SameSubnetThreshold = 10
```

You can also adjust other properties to control the workload tolerance for failover. Adjusting delay controls how often heartbeats are sent between the clustered node. The default setting is 1 second and the maximum setting is 2 seconds. Set the **SameSubnetDelay** value to 1. Threshold controls how many consecutive heartbeats can be missed before the node considers its partner to be unavailable and triggers the failover process. The default threshold is 5 heartbeats and the maximum is 120 heartbeats. It is the combination of delay and threshold that determines the total elapsed time during which clustered Windows nodes can lose communication before triggering a failover. When the clustered nodes are in different subnets, they are called **CrossSubnetDelay** and **CrossSubnetThreshold**. Set the **CrossSubnetDelay** value to 2 and the **CrossSubnetThreshold** value to 20.

Note: Recommended values for WSFC hearbeats settings are now defaults in Windows Server 2016 and above.

VMware vSphere® Virtual Volumes™ Support for WSFC

ESXi 7.0 supports VMware vSphere® Virtual Volumes™ storage and up to 5 node WSFC clusters. The storage array must support SCSI3-PRs at the subsidiary LUN level.

- ESXi 7.0 supports vVols Storage for Windows Server 2012 and above releases.
- Only Cluster-across-box (CAB) is supported.
- WSFC on vVols can work with any type of disk, "Thin" as well as "Thick"-provisioned disks.
- This feature enables customers to move away from using pRDM.
- WSFC on vVols supports vSphere HA, DRS and vMotion.
- The underlying transport protocol can be FC, SCSI or FCoE.
- Cluster-in-a-box (CIB) and a mixture of CAB and CIB is not supported.
- N+1 cluster configuration, in which one ESXi host has virtual machines which are secondary nodes and one primary node is a physical box is not supported.

vSphere WSFC Setup Limitations

Before you set up WSFC in a virtual envirioment, review the list of functions that are not supported for this release, and requirements and recommendations that apply to your configuration.

The following environments and functions are not supported for WSFC setups with this release of vSphere:

- Using VMDKs on NFS datastore as a shared disk resource for WSFC.
- Mixed environments, such as configurations where one cluster node is running a different version of ESXi than another cluster node.
- vSphere Fault Tolerance (FT).
- Migration with vMotion® of clustered virtual machines using vRDMs.
- N-Port ID Virtualization (NPIV)
- ESXi hosts or clusters that have memory overcommitment are not suitable for deploying WSFC virtual machines. Memory overcommitment can cause virtual machines to stall for short durations. This can be significantly disruptive as the WSFC clustering mechanism is time-sensitive and timing delays can cause the virtual machines to behave incorrectly.
- Suspend or resume of a VM, node of a WSFC.
- Storage spaces are not supported with Failover clustering on Windows 2012 and above.

- VM configurations changes:
  - Hot adding memory.
  - Hot adding CPU.
  - Increasing the size of a shared disk.
  - Pausing or resuming the virtual machine state. This I/O intensive operation is disruptive of the timing sensitive WSFC clustering software.
- Sharing disks between virtual machines without a clustering solution may lead to data corruptions

WSFC and Booting from a SAN

You can boot a VM from a SAN, node of a WSFC.

Booting from a SAN is complex. Problems that you encounter in physical environments extend to virtual environments. For general information about booting from a SAN, see the *vSphere Storage* documentation.

Follow these guidelines when you place the boot disk of a virtual machine on a SAN-based VMFS volume:

- Consider the best practices for boot-from-SAN that Microsoft publishes in the following knowledge base article: http://support.microsoft.com/kb/305547/en-us.
- Test clustered configurations in different failover scenarios before you put them into production environments.

Cluster Virtual Machines Across Physical ESXi Hosts

You can create a WSFC cluster that consists of two or more virtual machines on two ESXi or more hosts. Use this method for production deployments.

A cluster across physical hosts requires specific hardware and software.

- Up to 5 nodes in a single WSFC is supported
- Supported shared storage configuration, such as RDM in physical compatibility mode, vVol, clustered VMDK. For more information, see Supported Shared Storage Configurations.

Clustered VMDK support for WSFC

vSphere 7.0 introduces support for the use of VMDKs on clustered datastore as shared disk resources for a WSFC. Using VMDKs reduces the extra overhead to manage the virtual disks compared to pRDMs.

Microsoft Clustering Service uses SCSI-3 PRs commands to coordinate access to a clustered disk resource. These commands (PR-IN and PR-Out) are emulated at VSCSI layer on a datastore. The feature requires support from the datastore perspective. A datastore configured to host clustered VMDKs is referred to as a clustered VMDK datastore in this document.

Activating Clustered VMDK Support

You can activate clustered VMDK support when you create a new VMFS6 datastore, or activate clustered VMDK on an existing VMFS6 datastore. Before activating clustered VMDK support, ensure all hosts connected to the datastore are using ESXi 7.0 or later and are managed by vCenter 7.0 or later. All hosts connected to the datastore must be managed

by the same vCenter while deactivating or activating the clustered VMDK flag on the datastore. Once the clustered VMDK flag is activated or deactivated, hosts can be managed by any vCenter with version 7.0 or later.

1. Navigate to any inventory object that is a valid parent object of a datastore, such as a host, a cluster, or a data center, and click the **Datastores** tab.
2. Right-click the parent object and select **Create a New Datastore**.
3. On the **New Datastore** page choose a device with the attribute **Clustered VMDK Supported** set to `Yes`. Create a VMFS6 version Datastore.
4. Once the Datastore is created go to the **Configure Datastore** tab.
5. Under **General** go to the **Datastore Capabilities** section. Click the `Enable` button for **Clustered VMDK**.
6. Once activated, you can use the **Disable** button to deactivate clustered VMDK. Disable will not work if there are any WSFC VMs using clustered VMDKs on the datastore. All virtual machines with shared disks on the datastore must be powered off.

Configuration Maximums for Clustered VMDK Support

Configuration Maximums for Clustered VMDK support.

Configuration	Maximum
Max number of VMs in a single WSFC cluster	5
Max number of WSFC clusters (multi-cluster) running on the same set of ESXi hosts	3
Max number of clustered VMDKs per ESXi host	128

Recommendations for using Clustered VMDKs with WSFC

Follow these recommendations when using Clustered VMDKs with WSFC.

1. Do not present LUNs used for clustered VMDKs to ESXi hosts unless the host is configured with ESXi 7.0. This might cause slow boot times, hostd to become unresponsive and other issues. A host with a version lower than ESXi 7.0 cannot mount a clustered VMDK datastore. This is because the ESXi hosts on which WSFC VMs run must have physical SCSI-3 WEAR type reservation on the LUN.
2. Make sure that all VMs hosting nodes of WSFC are migrated off or powered off properly before removing it from a clustered VMDK datastore to ensure the resources, like heartbeat (HB) slots, are freed. If a VM fails or there is an APD on the clustered VMDK datastore during power-off, always power on and power off before removing the VM from a cluster.
3. Do not combine clustered and non-clustered VMDKs on the same clustered datastore. Although VMs that are using non-shared disks on a clustered datastore will continue to work normally and support all operations such as snapshot and clone.
4. Do not keep clustered VMDKs for different clusters on the same shared datastore. Use a different clustered datastore for different WSFC clusters.
5. Set vHardware (virtual compatibility) to vSphere 7.0 while using the clustered VMDK feature.

Requirements for using Clustered VMDKs with WSFC

You must follow these requirements when using Clustered VMDKs with WSFC.

1. You must set the Windows Cluster Parameter **QuorumArbitrationTimeMax** to 60.
2. The physical disk that virtual disks are stored on must support ATS SCSI commands.

3. The physical disk must support SCSI-3 Persistent Reservations, specifically Write Exclusive All Registrants (WEAR) type reservations.
4. VMDKs must be Eager Zeroed Thick Provisioned.
5. Storage devices can be claimed by VMware Native Multipathing Plugin (NMP) or by any other third-party MultiPathing Plugin (MPP). Check with vendors regarding the support for Clustered VMDK before using a vendor's third-party MultiPathing Plugin (MPP).

Limitations of Clustered VMDK support for WSFC

Clustered VMDK support is only possible with the following limitations:

1. Cluster in a Box (CIB) configuration is not supported.
2. Spanned VMFS datastores cannot store clustered VMDKs.
3. A physical LUN with a clustered datastore cannot have any additional VMFS datastores.
4. On-line Storage vMotion and snapshots are not supported.
5. Only disks with 512 sector size are supported.
6. VMFS5 and earlier are not supported for storing clustered VMDKs.
7. Only datastores connected through Fibre Channel (FC) are supported in this release.
8. Clustered VMDK datastore cannot be used as an ESXi installation disk.
9. Diagnostic partition is not supported on disks that are marked clustered.
10. SCSI-2 reservations are not supported on clustered VMDKs.
11. Hot expansion of a VMDK that is associated with a clustered VM is not supported.
12. A mix of clustered VMDKs with other types of clustered disks such as pRDMs or vVol in the same WSFC is not supported.
13. Moving more than one node of WSFC to the same ESXi host is not allowed and causes vMotion to fail. You must use anti-affinity DRS Rules to separate VMs and nodes of the cluster on different ESXi hosts.
14. Cloning and Fault Tolerance are not supported.

Create the First Node for WSFC Clusters Across Physical Hosts

To create the first node, you create and configure a virtual machine and install a guest operating system on the virtual machine.

1. Open the vSphere Client and connect to the vCenter Server system.

   Use the user name and password of the user who will have administrator permissions on the virtual machine.
2. In the vSphere Client, right-click the host and select **New Virtual Machine**.
3. Proceed through the wizard to create the virtual machine.

Page	Action
Creation type	Select **Create a new virtual machine**.
Name and folder	Enter a name and select a location.
Compute resource	Select a cluster, host, vApp or resource pool to run this virtual machine.
Storage	Select a datastore as the location for the virtual machine configuration file and the virtual machine disk (`.vmdk`) file.
Compatibility	The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.
Guest operating system	Select the guest operating system that you intend to install.
Customize hardware	Select virtual hardware, advanced virtual machine options, and SDRS rules if required or applicable.

Page	Action
Ready to Complete	Review your selections.

4. Click **Finish** to complete creating the virtual machine.

   Note: Do not add shared cluster disks at this time.

5. Install a Windows Server operating system on the virtual machine.

Create Additional Nodes for a WSFC Across Physical Hosts

To create additional nodes in a cluster of virtual machines across physical hosts, you can create a template from the the first virtual machine and use it to deploy additional virtual machines or use the procedure outlined previously to manually create additional VMs onto another ESXi host.

CAUTION: If you clone a virtual machine with an RDM setup, the cloning process converts the RDMs to virtual disks. Unmap all RDMs before cloning, and remap them after cloning is complete.

CAUTION: If you clone a virtual machine with clustered VMDKs, unmap all clustered VMDKs before cloning, and remap them after cloning is complete.

CAUTION: Use Windows sysprep operations before cloning to a template.

1. In the vSphere Client, right-click the first virtual machine you created and select **Clone** > **Clone to Template**.
2. Proceed through the wizard to create the virtual machine template.

Page	Action
Name and folder	Enter a name (for example, Node2_Template) and select a location.
Compute Resource	Select the host or cluster where you will run the virtual machine.
Disk Format	Select **Same format as source**.
Storage	Select a datastore as the location for the virtual machine configuration file and the `.vmdk` file.
Ready to Complete	Click **Finish** to create the virtual machine template.

3. Right-click the virtual machine template and select **Deploy VM from this Template**.
4. Proceed through the deployment wizard to deploy the virtual machine.

Page	Action
Name and folder	Enter a name (for example, Node2) and select a location.
Compute resource	Select the host or cluster where you will run the virtual machine.
Disk Format	Select **Same format as source**.
Datastore	Select a datastore as the location for the virtual machine configuration file and the `.vmdk` file.
Clone options	Select **Customize the operating system**.

5. Select a new guest operating system from the list.
   a) Click the **Create a new specification** button to add a new guest operating system. Proceed through the **New VM Guest Customization Spec** wizard.
   b) Click **Finish** to exit the wizard.
6. Click **Finish** to deploy the virtual machine.

Add Hard Disks to the First VM, first node of a WSFC, for Clusters Across Physical Hosts with pRDMs

In an WSFC cluster with shared disk, storage disks are shared between nodes.

Before you add hard disks to the first node, complete the following tasks:

- If you are using physical compatibility mode RDMs, ask your SAN administrator for the location of unformatted SAN LUNs. The hard disks you create in this task must point to SAN LUNs.
- If you are using vVols storage for shared disk, please see *Add Hard Disks to the First Node for Clusters Across Physical Hosts with VMware vSphere® Virtual VolumesTM*.
- If you are using Clustered VMDKs on VMFS datastores, please see *Add Hard Disks to the First Node for Cluster Across Physical Hosts with Clustered VMDKs on VMFS datastores*.

Note: Use RDMs in physical compatibility mode.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Physical**. Click **OK**.

   Note: LSI SAS is supported, but VMware Paravirtual is recommended.
4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**.
5. Click the **New device** drop-down menu, select **RDM Disk**.
6. Select an unformatted LUN and click **OK**.
7. Expand **New Hard disk** and select a datastore for **Location**.

   This datastore must be on shared storage because you need a single shared RDM file for each shared disk.
8. Select **Physical** as the compatibility mode.
9. Select the newly created SCSI controller in step 2, for virtual device node (for example, select **SCSI (1:0)**).

   Note: This must be a new SCSI controller. You cannot use SCSI 0. SCSI controller 0 is reserved for boot disks and disks which should not be shared
10. Click **OK**.

    The wizard creates a new hard disk.

Add Hard Disks to the First Node of a WSFC Across Physical Hosts with vVols

In an WSFC cluster, storage disks are shared between nodes.

Before you add hard disks to the first node, complete the following tasks:

- Use HW Version 13 or later. See Virtual Volumes (vVols) now supports WSFC.
- Prepare vVol deployment. See *vSphere Storage* documentation for more information.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Physical**. Click **OK**.

   Note: LSI SAS is supported, but VMware Paravirtual is recommended.
4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**
5. Click the **New device** drop-down menu, select **New Hard Disk**.
6. Expand **New Hard disk** and select the disk size required.
7. Select a datastore for **Location**.

   This datastore must be on shared vVols storage.

8. Under Disk Provisioning, select either Thick or Thin Provision.
9. Expand the New Hard Disk.
10. Select the newly created SCSI controller in step 2, for virtual device node (for example, select **SCSI (1:0)**).

    Note: This must be a new SCSI controller. You cannot use SCSI 0.
11. Click **OK**.

    The wizard creates a new hard disk.

Add Hard Disks to First Node for Cluster Across Physical Hosts with Clustered VMDKs on VMFS

Add hard disks to the first node for cluster across physical hosts with clustered VMDKs on VMFS datastores.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Physical**. Click **OK**.

    Note: LSI SAS is supported, but VMware Paravirtual is recommended.
4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**
5. Click the **New device** drop-down menu, select **New Hard Disk**.
6. Expand **New Hard disk** and select the disk size required.
7. Select a datastore for **Location**.

    This datastore must be the datastore with clustered VMDK flag enabled.
8. Under Disk Provisioning, select **Thick Provision with Eager zeroed**.
9. Select the newly created SCSI controller in step 2, for virtual device node (for example, select **SCSI (1:0)**).

    Note: This must be a new SCSI controller. You cannot use SCSI 0.
10. Click **OK**.

    The wizard creates a new hard disk.

Add Hard Disks to Additional Nodes for Clusters Across Physical Hosts

To allow shared access to disk resources, point to existing disks on the VM, the first node of a WSFC cluster. Use the same SCSI IDs while assigning disks to all additional nodes.

Before you begin, obtain the following information:

- Obtain SCSI IDs for all virtual disks to be shared.
- Obtain disk file path on datastore for all shared disks.

Note: The procedure for clustered VMDK, pRDMs and vVol is the same.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Physical**. Click **OK**.

    You must select same SCSI controller type, for example VMware Paravirtual, that you selected for the first virtual machine's shared storage disks.

    Note: LSI SAS is supported, but VMware Paravirtual is recommended.

4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**
5. Click the **New device** drop-down menu, select **Existing Hard Disk**.
6. In **Disk File Path**, browse to the location of the disk to be shared specified for the first node.
7. Expand **New Hard disk**.
8. Select the same SCSI ID you chose for the first virtual machine's shared storage disks, (for example, select **SCSI (1:0)**).

   Note: The disk SCSI ID for this virtual machine's shared storage must match the corresponding SCSI ID for the first virtual machine.
9. Click **OK**.

Use WSFC in an vSphere HA and vSphere DRS Environment

When you use WSFC in a vSphere High Availability (vSphere HA) or vSphere Distributed Resource Scheduler (DRS) environment, you must configure your hosts and virtual machines to use certain settings. All hosts that run WSFC virtual machines must be managed by a vCenter Server system.

VMware vSphere 7.0 provides support for vMotion of a VM, node of a WSFC.

Enable vSphere HA and vSphere DRS in ESXi

ESXi hosts that are running WSFC virtual machines can be part of a vSphere cluster with both vSphere HA and vSphere DRS enabled. You can enable vSphere HA and vSphere DRS in the Cluster Settings dialog box.

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Services**, select **vSphere DRS** and click **Edit**.
4. Select the **Turn ON vSphere DRS** and **Turn on vSphere HA** check boxes.
5. Click **OK**.

Create VM-VM Affinity Rules for WSFC Virtual Machines

For WSFC virtual machines in a cluster, you must create VM-VM affinity or anti-affinity rules. VM-VM affinity rules specify which virtual machines should be kept together on the same host (for example, a cluster of WSFC virtual machines on one physical host). VM-VM anti-affinity rules specify which virtual machines should be kept apart on different physical hosts (for example, a cluster of WSFC virtual machines across physical hosts).

For a cluster of virtual machines on one physical host, use affinity rules.

Note: Do not use a cluster on one physical host for production deployment.

For a cluster of virtual machines across physical hosts, use anti-affinity rules.

Note: vMotion is supported for a virtual machines, nodes of a WSFC, across physical ESXi hosts.

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Configuration**, click **VM/Host Rules**.
4. Click **Add**.
5. In the **Create VM/Host Rule** dialog box, type a name for the rule.
6. From the **Type** drop-down menu, select a rule.
   - For a cluster of virtual machines on one physical ESXi host, select **Keep Virtual Machines Together**.
   - For a cluster of virtual machines across physical ESXi hosts, select **Separate Virtual Machines**.
7. Click **Add**.
8. Select the two virtual machines to which the rule applies and click **OK**.
9. Click **OK**.

Set DRS Automation Level for WSFC Virtual Machines

Set the automation level of all virtual machines in an WSFC cluster to Partially Automated. When you set the vSphere DRS automation level for the virtual machine to Partially Automated, vCenter Server will perform initial placement of virtual machines when they are powered on and will provide migration recommendations for them.

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Services**, select **vSphere DRS** and click **Edit**.
4. Expand DRS Automation, under Virtual Machine Automation select the **Enable individual virtual machine automation levels** check box and click **OK**.
5. Under **Configuration**, select **VM Overrides** and click **Add**.
6. Click the **+** button, select the WSFC virtual machines in the cluster and click **OK**.
7. Click the Automation level drop-down menu, and select **Partially Automated**.
8. Click **OK**.

   Note: VMware recommends partially automated mode for WSFC virtual machines, but there is no technical restriction which prevents the setting for WSFC virtual machines to be fully automated. If the fully automated setting is used please tune WSFC advanced settings to prevent WSFC failover during vMotion.

Using vSphere DRS Groups and VM-Host Affinity Rules with WSFC Virtual Machines

You can set up two types of DRS groups: virtual machine DRS groups, which contain at least one virtual machine, and host DRS groups, which contain at least one host. A VM-Host rule establishes an relationship between a virtual machine DRS group and a host DRS group.

You must use VM-Host affinity rules because vSphere HA does not obey VM-VM affinity rules. This means that if a host fails, vSphere HA might separate clustered virtual machines that are meant to stay together, or vSphere HA might put clustered virtual machines that are meant to stay apart on the same host. You can avoid this problem by setting up DRS groups and using VM-Host affinity rules, which are obeyed by vSphere HA.

For a cluster of virtual machines on one physical host, all WSFC virtual machines must be in the same virtual machine DRS group, linked to the same host DRS group with the affinity rule "Must run on hosts in group."

For a cluster of virtual machines across physical hosts, all WSFC virtual machines must be in the same virtual machine DRS group and all hosts must be in the same host DRS group. The virtual machine and host DRS groups must be linked the affinity rule "Must run on hosts in group."

CAUTION: Limit the number of hosts to two when you define host DRS group rules for a cluster of virtual machines on one physical ESXi host. (This does not apply to clusters of virtual machines across physical ESXi hosts.) Since vSphere HA does not obey VM-VM affinity rules, virtual machines in the configuration could be spread across hosts during a vSphere HA recovery from host failure if more than two hosts are included in a host DRS group rule.

Create a Virtual Machine DRS Group (WSFC)

Before you can create a VM-Host affinity rule, you must create the host DRS group and the virtual machine DRS group that the rule applies to.

For both, a cluster of virtual machines on one physical host(CIB) and a cluster of virtual machines across physical hosts(CAB), create one virtual machine DRS group that contains all WSFC virtual machines. For example, VMGroup_1 contains WSFC_VM_1, WSFC_VM_2 … WSFC_VM_5.

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Configuration**, select **VM/Host Groups** and click **Add**.
4. In the **Create VM/Host Group** dialog box, type a name for the group.
5. Select **VM Group** from the **Type** drop down box and click **Add**.
6. Click the check box next to a virtual machine to add it. Continue this process until all desired virtual machines have been added.
   - For a cluster of virtual machines on one physical host, add all WSFC virtual machines to one group.
   - For a cluster of virtual machines across physical hosts, add all WSFC virtual machines to one group.
7. Click **OK**.

Create a Host DRS Group (WSFC)

Before you can create a VM-Host affinity rule, you must create the host DRS group and the virtual machine DRS group that the rule applies to.

For a cluster of virtual machines on one physical host, create one host DRS group that contains both the ESXi hosts. For example, HostGroup_1 contains ESXi_HOST_1, ESXi_HOST_2.

For a cluster of virtual machines across physical hosts, create one host DRS group that contains all the ESXi hosts. For example, HostGroup_1 contains ESXi_HOST_1 running WSFC_VM_1, ESXi_HOST_2 running WSFC_VM_2 …... ESXi_HOST_5 running WSFC_VM_5 and ESXi_HOST_6 as a standby host.

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Configuration**, select **VM/Host Groups** and click **Add**.
4. In the **Create VM/Host Group** dialog box, type a name for the group (for example, `HostGroup_1`).
5. Select **Host Group** from the **Type** drop down box and click **Add**.
6. Click the check box next to a host to add it. Continue this process until all desired hosts have been added.
7. Click **OK**.

Set up VM-Host Affinity Rules for DRS Groups (WSFC)

Create VM-Host affinity rules to specify whether the members of a selected virtual machine DRS group can run on the members of a specific host DRS group.

Create virtual machine DRS groups that contain one or more WSFC virtual machines as described in Create a Virtual Machine DRS Group (WSFC).

Create host DRS groups that contain one or more ESXi hosts, as described in Create a Host DRS Group (WSFC).

1. Browse to the cluster in the vSphere Client.
2. Click **Configure**.
3. Under **Configuration**, select **VM/Host Rules** and click **Add**.
4. In the **Create VM/Host Rule** dialog box, type a name for the rule.
5. From the **Type** menu, select **Virtual Machines to Hosts**.
6. Select the virtual machine DRS group and the host DRS group to which the rule applies. For example, select VMGroup_1 and HostGroup_1.
7. Select **Must run on hosts in group**.
8. Click **OK**.

vSphere WSFC Setup Checklist

When you set up a WSFC on VMware vSphere, see the checklists to configure your environment according to the requirements. You can also use the checklists to verify that your setup meets the requirements if you need technical support.

Requirements for Clustered Disks

Each type of clustered disk has its own requirements, depending on whether it is in a single-host cluster or multihost cluster.

Table 533: Requirements for Clustered Disks

Component	Single-Host Clustering	Multihost Clustering
Clustered VMDK	SCSI bus sharing mode set to virtual is not supported.	SCSI bus sharing mode set to physical is supported.
VMDK (In virtual compatibility mode)	SCSI bus sharing mode set to virtual is supported. (Not Recommended)	SCSI bus sharing mode set to Physical is not supported.
vRDM	Device type must be set to virtual compatibility mode. SCSI bus sharing mode must be set to virtual mode. A single, shared RDM mapping file for each clustered disk is required.	Not supported.
pRDM	Not supported.	RDM device type must be set to Physical compatibility mode during hard disk creation. SCSI bus sharing mode of vSCSI Controller hosting pRDM must be set to physical. A single, shared RDM mapping file for each clustered disk is required.
vVols storage	Not Supported.	SCSI bus sharing mode of vSCSI controller must be set to physical.
All types	All clustered nodes must use the same target SCSI ID (on the virtual SCSI adapter) for the same clustered disk. A separate virtual SCSI adapter must be used for clustered disks. Multiple virtual SCSI adapters for clustered disks (up to supported maximum) can be used to enhance performance. In this setup at least one controller should be dedicated to non-shared disk.	

Other Requirements and Recommendations

The following table lists the components in your environment that have requirements for options or settings.

Table 534: Other Clustering Requirements and Recommendations

Component	Requirement
Disk	Select Thick Provision with Eager zeroed during disk provisioning for VMDKs (for clustered VMDKs or VMDKs in virtual compatibility mode). For vVols select either thick or thin. Modify the .vmx file for the WSFC VMs to add these lines: • `scsiX.returnNoConnectDuringAPD = "TRUE"` • `scsiX.returnBusyOnNoConnectStatus = "FALSE"` • Where X is the boot device SCSI bus controller ID number. By default, X is set to 0. The only disks that you should not create with the `Thick Provision` option are RDM files (both physical and virtual compatibility mode). Disk I/O timeout is 60 seconds or more (`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue`).
Windows	Use: • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016

Component	Requirement
	• Windows Server 2019 with vSphere 6.7 Update 3 • Windows Server 2022 with vSphere 7.0 For Windows Server 2012 and above, you can use up to five cluster nodes. **Note:** If you recreate the cluster, this value might be reset to its default, so you must change it again. The cluster service must restart automatically on failure (first, second, and subsequent times). **Note:** Windows Server 2008 and 2008 R2 have reached the end of extended support (no regular security updates). Consider the vendor support ability while hosting a WSFC on VMware vSphere.
ESXi	Do not overcommit memory. Set the **Memory Reservation** (minimum memory) option to the same as the amount of memory assigned to the virtual machine. ESXi uses a different technique to determine if Raw Device Mapped (RDM) LUNs are used for WSFC cluster devices, by introducing a configuration flag to mark each device as "perennially reserved" that is participating in an WSFC cluster. For ESXi hosts hosting passive WSFC nodes with RDM LUNs, use the esxcli command to mark the device as perennially reserved: `esxcli storage core device setconfig -d <naa.id> --perennially-reserved=true`. See KB 1016106 for more information. Clustered VMDK in ESXi 7.0 must also be marked as perennially reserved.
Multipathing	Contact your multipathing software vendor for information and support of non-VMware multipathing software in vSphere.

Required Information for Technical Support

The following table lists the files and settings to collect if you require technical support. Technical support uses these files and settings to analyze issues with a WSFC setup.

Note: Verify that your setup complies with the checklists in Table 1 and Table 2 before you contact technical support.

Table 535: Information Required by Technical Support

File or Information	Description or Location
`vm-support tarball`	Contains the vmkernel log, virtual machine configuration files and logs, and so on.
Application and system event logs of all virtual machines with the problem	
Cluster log of all virtual machines with the problem	`%ClusterLog%`, which is usually set to `%SystemRoot%\cluster\cluster.log` or use `Get-ClusterLog Powershell CMdlet`
Disk I/O timeout	`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\TimeOutValue`
vSphere Client display names and Windows NETBIOS names of the virtual machines experiencing the problem	
Date and time that the problem occurred	
SAN configuration of the ESXi system	Details about LUNs, paths, and adapters.
(Optional) Memory dump of the virtual machine	Required if a guest virtual machine fails (a blue screen appears with an error message).

Cluster Virtual Machines on One Physical Host

You can create an WSFC cluster with up to five nodes on a single ESXi host.

Note: For production deployments, do not set up a WSFC on VMs residing on a single ESXi host.

Note: Windows Server 2012 and above systems support up to five nodes (virtual machines). For supported guest operating systems see Table 4.

Create the First Node of a WSFC on One Physical ESXi Host

To create the first node, you create and configure a virtual machine and install a guest operating system on the virtual machine.

1. Open the vSphere Client and connect to the vCenter Server system.

   Use the user name and password of the user who will have administrator permissions on the virtual machine.

2. In the vSphere Client, right-click the host and select **New Virtual Machine**.

3. Proceed through the wizard to create the virtual machine.

Page	Action
Creation type	Select **Create a new virtual machine**.
Name and folder	Enter a name and select a location.
Compute resource	Select a cluster, host, vApp or resource pool to run this virtual machine.
Storage	Select a datastore as the location for the virtual machine configuration file and the virtual machine disk (`.vmdk`) file.
Compatibility	The host or cluster suports more than one VMware virtual machine version. Select a compatibility for the virtual machine.
Guest operating system	Select the guest operating system that you intend to install.
Customize hardware	Select virtual hardware, advanced virtual machine options, and SDRS rules.
Ready to Complete	Review your selections.

4. Click **Finish** to complete creating the virtual machine.

   Note: Do not add shared cluster disks at this time.

5. Install a Windows Server operating system on the virtual machine.

Create Additional Nodes for Clusters on One Physical Host

Create a template from the first virtual machine and deploy the second node from that template. You can have up to five nodes on Windows Server 2012 or later.

Note: For a clean template, use Windows Sysprep.

CAUTION: If you clone a virtual machine with an RDM setup, the cloning process converts the RDMs to virtual disks. Unmap all RDMs before cloning, and remap them after cloning is complete.

1. In the vSphere Client, right-click the first virtual machine you created and select **Clone** > **Clone to Template**.

2. Proceed through the wizard to create the virtual machine template.

Page	Action
Name and folder	Enter a name (for example, Node2_Template) and select a location.
Compute Resource	Select the host or cluster where you will run the virtual machine.
Disk Format	Select **Same format as source**.
Storage	Select a datastore as the location for the virtual machine configuration file and the `.vmdk` file.
Ready to Complete	Click **Finish** to create the virtual machine template.

3. Right-click the virtual machine template and select **Deploy VM from this Template**.
4. Proceed through the deployment wizard to deploy the virtual machine.

Page	Action
Name and folder	Enter a name (for example, Node2) and select a location.
Compute resource	Select the host or cluster where you will run the virtual machine.
Disk Format	Select **Same format as source**.
Datastore	Select a datastore as the location for the virtual machine configuration file and the `.vmdk` file.
Clone options	Select **Customize the operating system**.

5. Select a new guest operating system from the list.
   a) Click the **Create a new specification** button to add a new guest operating system. Proceed through the **New VM Guest Customization Spec** wizard.
   b) Click **Finish** to exit the wizard.
6. Click **Finish** to deploy the virtual machine.

Add Hard Disks to the First Node for Clusters on One Physical Host

In an WSFC cluster, storage disks are shared between nodes. You set up a quorum disk and at least one shared storage disk.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Virtual**. Click **OK**.

   Note: LSI SAS is supported, but VMware Paravirtual is recommended.
4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**
5. Click the **New device** drop-down menu, select **Hard Disk**.
6. Expand **New Hard disk** and select the disk size required.
7. Select a datastore for **Location**.
8. Under Disk Provisioning, select **Thick Provision with Eager zeroed**.
9. Select the newly created SCSI controller in step 2, for virtual device node (for example, select **SCSI (1:0)**).

   Note: This must be a new SCSI controller. You cannot use SCSI 0.
10. Click **OK**.

    The wizard creates a new hard disk.

Add Hard Disks to Additional Nodes for Clusters on One Physical Host

To allow shared access to clustered services and data, use **Add an Existing disk** on the second VM to point to the disks from the first VM that should be shared. Use the same SCSI IDs.

Before you begin, obtain the following information:

- Obtain SCSI IDs for all virtual disks to be shared.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Virtual**. Click **OK**.

   Note: LSI SAS is supported, but VMware Paravirtual is recommended.
4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**
5. Click the **New device** drop-down menu, select **Existing Hard Disk**.
6. In **Disk File Path**, browse to the location of the disk to be shared specified for the first node.
7. Expand **New Hard disk**.
8. Select the same SCSI ID you chose for the first virtual machine's shared storage disks, (for example, select **SCSI (1:0)**).

   Note: The disk SCSI ID for this virtual machine's shared storage must match the corresponding SCSI ID for the first virtual machine.
9. Click **OK**.

Cluster Physical and Virtual Machines

You can create an WSFC cluster in which each physical server has a corresponding virtual machine. This type of configuration is known as a standby host cluster.

A standby host cluster has specific hardware and software requirements.

- Network configuration should be consistent between a physical and virtual node of a WSFC. Ensure that all required VLANs are available to ESXi hosts, hosting a virtual node of a WSFC cluster.
- Use RDMs in physical compatibility mode. You cannot use virtual disks or RDMs in virtual compatibility mode for shared storage.
- Use the STORport Miniport driver for the Fibre Channel (FC) HBA (QLogic or Emulex) in the physical Windows machine.
- Do not run multipathing software in the physical or virtual machines.
- Use only a single physical path from the host to the storage arrays in standby host configurations.

Create the First Node for a Cluster of Physical and Virtual Machines

The first node in a standby host setup is a physical machine.

For information about setting up a physical machine that participates in an WSFC cluster, see the Failover Cluster for Windows documentation.

- Set up the physical machine using the settings listed in the table.

Component	Requirement
Windows Cluster Administrator application	Advanced minimum configuration if Windows 2012 is used.
Storage	Access to the same storage on a SAN as the ESXi host on which the corresponding virtual machine will run.
Operating system	Installed on each physical machine.

Create the Second Node for a Cluster of Physical and Virtual Machines

To create the second node, you set up a virtual machine, a second node of a WSFC cluster, where the first node is a physical server.

Before you begin, make sure that the shared storage that is visible from the physical machine that you configured in Create the First Node for a Cluster of Physical and Virtual Machines is also visible from the ESXi host.

1. Open the vSphere Client and connect to the vCenter Server system.

   Use the user name and password of the user who will have administrator permissions on the virtual machine.
2. In the vSphere Client, right-click the host and select **New Virtual Machine**.
3. Proceed through the wizard to create the virtual machine.

Page	Action
Creation type	Select **Create a new virtual machine**.
Name and folder	Enter a name and select a location.
Compute resource	Select a cluster, host, vApp or resource pool to run this virtual machine.
Storage	Select a datastore as the location for the virtual machine configuration file and the virtual machine disk (`.vmdk`) file.
Compatibility	The host or cluster suports more than one VMware virtual machine version. Select a compatibility for the virtual machine.
Guest operating system	Select the guest operating system that you intend to install.
Customize hardware	Select virtual hardware, advanced virtual machine options, and SDRS rules.
Ready to Complete	Review your selections.

4. Click **Finish** to complete creating the virtual machine.
5. Install a Windows Server operating system on the virtual machine.

Add Hard Disks to the Second Node for a Cluster of Physical and Virtual Machines

When you add hard disks to the second node, you set up the disks to point to the shared storage disks for the first node. The setup allows shared access to clustered disks.

1. In the vSphere Client, select the newly created virtual machine, right-click and select **Edit Settings**.
2. Click the **New device** drop-down menu, select **SCSI Controller**.
3. In new SCSI Controller, select **VMware Paravirtual** and set **SCSI Bus Sharing** to **Physical**. Click **OK**.

   Note: LSI SAS is supported, but VMware Paravirtual is recommended.
4. Select the newly created virtual machine in step 1, right-click and select **Edit Settings**
5. Click the **New device** drop-down menu, select **RDM Disk**.
6. Select an unformatted LUN and click **OK**.
7. Expand **New Hard disk**.
8. Select a datastore for **Location**.

   This datastore must be on shared storage because you need a single shared RDM file for each shared disk.
9. Select compatibility mode **Physical**.
10. Select the newly created SCSI controller in step 2, for virtual device node (for example, select **SCSI (1:0)**).

    Note: This must be a new SCSI controller. You cannot use SCSI 0.
11. Click **OK**.

    The wizard creates a new hard disk.

Install Microsoft Cluster Service

After you set up the first and second nodes, you must configure Microsoft Failover Clustering.

See Microsoft's documentation for creating and configuring server clusters on the Microsoft Web site.

In complex storage solutions, such as an FC switched fabric, a storage unit might have a different identity (target ID or raw disk ID) on each computer in the cluster. Although this is a valid storage configuration, it might cause a problem when you add a node to the cluster.

Create Additional Physical-Virtual Pairs

If you have additional physical machines, you can create additional clusters for each.

1. On the ESXi host, set up an additional virtual machine for the physical machine.
2. Cluster the physical machine with the new virtual machine.

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2005–2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

vmware®
by Broadcom